



Traditional Credit Union (TCU)

www.tcu.com.au

ABN 50 087 650 922

AFSL/Australia Credit Licence 244 255

BSB number 704-062

Version 23: 1 November 2025

Account Information and Access Facility Terms and Conditions

Personal & Business Accounts

The Account and Access Facility is issued by:

Traditional Credit Union Limited

ABN 50 087 650 922

Australian Financial Services Licence 244 255

HOW TO CONTACT US

In person Visit us at any branch – see our website for our branch details.
Telephone: 08 8999 0777
Email: info@tcu.com.au
Postal Address: PO Box 40425
Casuarina NT 0811
Website: www.tcu.com.au

TO REPORT THE LOSS, THEFT OR UNAUTHORISED USE OF YOUR CARD

- **in Australia – for CueCard and Visa**
call the Hotline on 1800 621 199, 24 hours a day, everyday.
Please also contact us to report the loss, theft or unauthorised use.
- **overseas – for CueCard and Visa**
Please call us in Australia during our office hours.
call +612 9959 7480, 24 hours a day, everyday.

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. You can download a copy of the Customer Owned Banking Code of Practice at: www.customerownedbanking.asn.au

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.

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 www.tcu.com.au.

FINANCIAL CLAIMS SCHEME

The Financial Claims Scheme (FCS) protects depositors through the provision of a guarantee on deposits (up to the cap) held in authorised deposit-taking institutions (ADIs) incorporated in Australia and allows quick access to their deposits if an ADI becomes insolvent.

The Credit Union is an ADI. Depositors with the Credit Union may be entitled to receive a payment from the FCS, subject to a limit per depositor. For further information about the FCS visit the website: <http://www.fcs.gov.au>.

TABLE OF CONTENTS

Account Operations	5
What Is The Account and Access Facility?	5
How Do I Open An Account?	5
Proof Of Identity Required	5
What Accounts Can I Open?	5
Joint Accounts	5
Trust Accounts	6
What Fees And Charges Are There?	6
What Interest Can I Earn On My Account?	6
What Are The Taxation Consequences?	6
Disclosing Your Tax File Number	7
Third Party Access	7
Making Deposits To The Account	7
Deposits Using Electronic Equipment	7
Depositing Cheques Drawn on Australian Banks	7
Withdrawing Or Transferring From The Account	8
Debiting Transactions Generally	8
Over The Counter Withdrawals	8
Withdrawals Using Our Corporate Cheques	8
Transaction Limits	9
Overdrawing An Account	9
Sweep Facility	9
Account Statements	9
What Happens If My Details Change?	9
Dormant Accounts	9
Account Combination	10
Closing Accounts, Cancelling Access Facilities & Blocking Access or Transactions	10
Notifying Changes	10
How We Send Notices & Statements	11
Direct Debit	11
Electronic Access Facilities and ePayments Conditions of Use	12
Complaints	25
Verified by Visa	26
Using the VBV Visa Service	26
Privacy	26
Termination of Verified by Visa	26
Participating Online Merchants	26
Exclusion of Liabilities	27
Your Conduct	27

Your Liability 27

Errors 27

Summary of Accounts & Availability of Access Facilities..... 28

Transactional and Savings Accounts 28

Investments (Term Deposits) 31

Business Accounts 31

Notes For Summary of Accounts & Availability of Access Facilities 32

ACCOUNT OPERATIONS

WHAT IS THE ACCOUNT AND ACCESS FACILITY?

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

- CueCard
- Visa Debit Card
- BPAY® (registered to BPAY® Pty Ltd ABN 69 079 137 518)
- Telephone, internet and mobile banking
- EFTPOS and ATM access
- direct debit requests.

Please refer to the *Summary of Accounts & Availability of Access Facilities* section 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 the Credit Union before we can issue the Account and Access Facility to you. To become a member, you will need to subscribe for a share in the Credit Union.

PROOF OF IDENTITY REQUIRED

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

In most cases you can prove your identity by showing us a government issued photo identity document, such as a driver's licence or passport. If you do not have photo ID, please contact us to discuss what other forms of identification may be acceptable. In some circumstances we may verify your identity electronically using information you provide.

WHAT ACCOUNTS CAN I OPEN?

When we issue you with the Account and Access Facility, you have access to the applied account. Check the *Summary of Accounts & Availability of Access Facilities* section for the different account types available, any special conditions for opening, and the features and benefits of each account type.

JOINT ACCOUNTS

A joint account is an account held by two or more persons. The important legal consequences of holding a joint account are:

- the right of survivorship – when one joint holder dies, the surviving joint holders automatically take the deceased joint holder's interest in the account (for business accounts different rules may apply - see Note below)
- joint and several liability – if the account is overdrawn, each joint holder is individually liable for the full amount owing.

You can operate a joint account on a 'joint operation' or 'individual operation' basis:

- 'joint operation' means 2 or more joint holders must authorise any withdrawal, payment or transfer from the account (including a direct debit)
- 'individual operation' means any one joint holder can authorise any withdrawal, payment or transfer from the account (including a direct debit).

By default, new joint accounts will be opened on an individual operation basis unless the joint holders instruct otherwise in the account opening application. The joint holders can jointly change account operating instructions in writing at any time.

However, irrespective of the joint account operating instructions, any one joint holder can instruct us to:

- change the account operation to joint operation by all joint holders only; or
- suspend the account to allow the joint holders time to reach agreement about dispersal of the account funds,

in which case these instructions will remain in effect until all joint holders agree otherwise.

We may also change the account operation to joint operation by all joint holders only, if we become aware of a dispute between the joint holders, or of the bankruptcy of any joint holder.

Please note that some access facilities (such as access cards) may not be available if the joint account operates on a joint operation basis.

Irrespective of the joint account operating instructions, all joint account holders will need to provide instructions to:

- close the account
- withdraw or redeem a term deposit prior to maturity
- appoint a third-party signatory to the account
- request a transaction limit increase
- change the method or address for delivery of statements or notices in relation to the joint account – this does not prevent a joint holder changing their method or address for delivery of statements or notices they receive individually, which may include in relation to the joint account.

The above applies to joint personal accounts. For joint business accounts, such as partnership accounts, we may accept and rely on different account operating instructions. Please contact us for information about joint business accounts.

Note: The right of survivorship does not automatically apply to joint business accounts, such as partnerships. A partner's interest in a business joint account would normally pass to beneficiaries nominated in the partner's will or next-of-kin if there is no will.

If you are operating a business partnership joint account, you should obtain your own legal advice to ensure your wishes are carried out.

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; and
- 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 *Interest, 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.

WHAT INTEREST CAN I EARN ON MY ACCOUNT?

Our Interest, Fees and Charges brochure provides information about our current deposit and savings interest rates. The brochure also discloses how we calculate and credit interest to your account. 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.

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 the Account and Access Facility, we will ask you whether you want to disclose your Tax File Number (TFN) 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 will deduct withholding tax 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 (a signatory) to operate on your account. However, we will need to verify this person's identity before they can access your account.

You are responsible for all transactions the signatory carries out on your account. **You should ensure that the person you authorise to operate on your account is a person you trust fully.**

For personal accounts, a signatory's authority is limited to:

- carrying out withdrawals, payments or transfers from the account; and
- making enquiries about account balances and transactions on the account, including any debit balance or available credit on a transactional account.

For business accounts please contact us about applicable signatory options.

You may revoke the signatory'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 our office [or 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

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

DEPOSITS USING ELECTRONIC EQUIPMENT

We are responsible for a deposit into a facility received by our electronic equipment, from the time you complete the deposit, subject to verification of the amount or amounts deposited.

If there is a discrepancy between the amount recorded as being deposited by the electronic equipment and the amount recorded by us as being received, we will contact you as soon as practicable about the difference.

Note that electronic deposits may not be processed on the same day.

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.

WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT

You can make withdrawals or transfers from the account:

- over the counter at our office [or any branch]
- by direct debit
- by cheque, if your account is linked to a cheque book
- by telephone banking
- by internet or mobile banking
- by BPAY to make a payment to a biller
- at selected ATMs, if your account is linked to an access card
- via selected EFTPOS terminals, if your account is linked to an access card (note that Merchants may impose restrictions on withdrawing cash)

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

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. Transactions will not necessarily be processed to your account on the same day.

We have the right to decline to accept your authorisation for any transaction if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give the authorisation. We may also delay or not process a transaction for any of the reasons set out in *Closing Accounts, Cancelling Access Facilities & Blocking Access or Transactions* on page 9. 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 that transaction.

OVER THE COUNTER WITHDRAWALS

Generally, you can make over-the-counter withdrawals in cash or by buying a Credit Union corporate cheque. Please check:

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

WITHDRAWALS USING OUR CORPORATE CHEQUES

This is a cheque the Credit Union draws payable to the person you nominate. You can purchase a corporate cheque from us for a fee: see the *Interest, Fees and Charges* 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, either generally or in relation to a particular facility. These transaction limits are set out in the *Interest, Fees, and Charges* 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.

We may, on application from you, agree to vary a transaction limit. We may also require you to apply for new transaction limits if you change any pass code. 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 electronic transactions. If you do not, we can dishonour the transaction and charge dishonour fees: see the *Interest, Fees and Charges* 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 *Interest, 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.

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 *Interest, Fees and Charges* brochure.

We recommend that you check your account statement as soon as you receive it. Immediately notify us of any unauthorised transactions or errors. Please refer to *How to Contact Us* on page 2 for our contact details.

WHAT HAPPENS IF MY DETAILS CHANGE?

You must let us know immediately if you change any of your personal or contact details including your name, address, email address or mobile phone number. You can update your contact details via internet banking or by contacting us (see *How to Contact Us* on page 2).

DORMANT ACCOUNTS

If no transactions are carried out on your account for at least 12 months (other than transactions initiated by the Credit Union, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep the account open. If you do not reply, we will treat your account as dormant.

Once your account becomes dormant, we may:

- charge a dormancy fee;
- stop paying interest or reduce the amount of interest

If your account remains dormant for 7 years we have a legal obligation to remit balances exceeding \$500 to the Australian Securities and Investment 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.

When you cease to be a customer, 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: Recovery of Debts from Customer Nominated Bank Accounts in receipt of Services Australia income support payments or Department of Veterans Affairs' payments and any successor Code (both when enforcing indebtedness owed to us and, to the extent the law permits, when facilitating enforcement by a third party judgment creditor).

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

CLOSING ACCOUNTS, CANCELLING ACCESS FACILITIES & BLOCKING ACCESS OR TRANSACTIONS

You can close the Account and Access Facility at any time. However, you will have to surrender any access card at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding electronic transactions and fees, if applicable.

You can cancel any access facility on request at any time.

We can close the Account and Access Facility in our absolute discretion by giving you at least 14 days' notice and paying you the balance of your account.

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 suspect fraudulent or illegal use of the account or access facility;
- if we suspect that a transaction may breach a law or sanction;
- 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.

NOTIFYING CHANGES

We may change fees, charges, interest rates and other conditions at any time. The following table sets when we will notify you of any change.

Type of change	Minimum 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 or debited to your account	20 days
Increasing your liability for losses relating to ePayments (see the ePayments Conditions of Use Section 3 on page 14 for a description of ePayments)	20 days
Imposing, removing or changing any periodic transaction limit relating to ePayments	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 or other direct communication (including by electronic means);
- notification on or with your next statement of account;
- notification on or with the next newsletter;
- advertisements in the local or national media;
- 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 and effectiveness of the method of notification.

If there is a change to, or introduction of a government charge that you directly or indirectly pay as part of your banking service, we will tell you about this reasonably promptly after the government notifies us, unless the government itself publicises the introduction or change.

HOW WE SEND NOTICES & STATEMENTS

To the extent permitted by law, we may send you notices and statements:

- by post, to the address recorded in our records or to a mailing address you nominate;
- by electronic means, including by email to an email address you have given us, SMS to a mobile phone number you have given us, or via our mobile banking app;
- by advertisement in the media or our website, for some notices only;
- by other means we agree with you.

We may, instead of sending you a notice or statement, post notices or statements to our website or internet banking service for you to retrieve. In that case, we will notify you via email or other electronic means, when information is available for you to retrieve.

We may charge a fee for providing paper statements or notices: see the *Interest, Fees and Charges* brochure.

You must ensure your address and other contact details, including email address and mobile phone number, are correct and up to date at all times.

DIRECT DEBIT

You can authorise a participating biller to debit amounts from your eligible account (using your BSB and account number), 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 take action within 1 business day to cancel the facility. We suggest that you also contact the biller. We will promptly investigate if you inform us that a direct debit was not authorised or is otherwise irregular. We suggest that you also contact 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 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.

ELECTRONIC ACCESS FACILITIES AND ePAYMENTS CONDITIONS OF USE

Section 1. INFORMATION ABOUT OUR ePAYMENT FACILITIES

You should follow the guidelines in the box below to protect against unauthorised use of your access cards, devices and pass codes. 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 About Protecting Your Access Cards, Devices and Pass Codes

- 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 device, or to report unauthorised use of your access card, BPAY® or telephone, internet or mobile banking.
- Immediately report lost, theft or unauthorised use or access (see How To Contact Us on page 2).
- 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 or save the pass code on any access card, mobile phone, computer or device, even if disguised.
- Never write the pass code on anything which is kept with or near any access card, mobile phone, computer or device.
- 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 any electronic equipment.
- Keep a record of the VISA card number and the VISA Card Hotline telephone number for your area with your usual list of emergency telephone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address, and ensure your contact details, including email address and mobile phone number, are correct and up to date at all times.
- ALWAYS access the telephone banking or internet banking service only using the OFFICIAL phone numbers and URL addresses.
- NEVER access internet banking via a link in an email, SMS or other electronic message.
- 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.

These ePayment Conditions of Use govern all electronic transactions made using any one of our access cards or facilities, listed below:

CueCard
Visa Card
BPAY®

Mobile Banking
Internet Banking
Telephone Banking

You can use any of these electronic access facilities to access an account, as listed in the *Summary of Accounts & Availability of Access Facilities* section.

CueCard

CueCard allows you to access your account at an ATM or EFTPOS terminal in Australia displaying the **CueCard logo**. We will provide you with a PIN to use with your CueCard. CueCard 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).

CueCard also allows you to access your account at an ATM or EFTPOS terminal overseas displaying the **Visa logo**.

We may choose not to give you a CueCard 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:

- 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 the Credit Union is not satisfactory or if you are under 18 years of age.

Important Information about Chargebacks for VISA Card

If you wish to dispute a Visa Card transaction you should notify us as soon as possible. Under the Visa Card scheme rules we can seek a refund of Visa Card purchases from the merchant's financial institution in certain circumstances, such as non-delivery of goods or services ordered, unauthorised purchases, or payments under a regular payment arrangement that you had already cancelled. This is called a 'chargeback'.

The Visa Card scheme rules impose strict timeframes on requesting chargebacks. We will need to investigate a disputed transaction to determine if we have a right to a chargeback. You must provide us with any information or material we request to investigate the transaction and support the chargeback request. If we determine that we have a right to a chargeback we will seek it without delay.

It is in your own interest to notify us as soon as possible if you become aware of circumstances which might entitle us to claim a chargeback on your behalf.

However, you should seek to resolve the issue with the merchant first.

Please note that we can only seek a chargeback where the Visa Card scheme rules apply to your use of the Visa card. In particular, chargebacks do not apply where the card is used for an EFTPOS payment (e.g. where you select payment from 'savings' or 'cheque') or for BPay payments.

Section 2. DEFINITIONS

- (a) **access card** means an ATM card, debit card or credit card and includes our Visa Card and CueCard.
- (b) **ATM** means automatic teller machine
- (c) **business day** means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned
- (d) **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
 - (iii) token issued by us that generates a pass code
- (e) **EFTPOS** means electronic funds transfer at the point of sale—a network for facilitating transactions at point of sale
- (f) **facility** means an arrangement through which you can perform transactions
- (g) **identifier** means information that a user:
 - (i) knows but is not required to keep secret, and
 - (ii) must provide to perform a transactionExamples include an account number or customer number.
- (h) **manual signature** means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet
- (i) **NPP** means the New Payments Platform operated by NPP Australia Limited
- (j) **NPP Payments** means electronic payments cleared and settled by participating financial institutions via the NPP
- (k) **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, or a phrase. Examples include:
 - (i) personal identification number (PIN)
 - (ii) internet banking password
 - (iii) telephone banking passwordA pass code does not include a number printed on a device (e.g. a security number printed on a credit or debit card).
- (l) **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 using your debit card or credit card details at predetermined intervals (eg. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.
- (m) **transaction** means a transaction to which these ePayment Conditions of Use apply, as set out in Section 3
- (n) **unauthorised transaction** means a transaction that is not authorised by a user
- (o) **user** means you or an individual you have authorised to perform transactions on your account, including:
 - (i) a third party signatory to your account
 - (ii) a person you authorise us to issue an additional card to.

Section 3. TRANSACTIONS

- 3.1. These ePayment Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:
 - (a) initiated using electronic equipment, and
 - (b) not intended to be authenticated by comparing a manual signature with a specimen signature.

- 3.2. Without limiting clause 3.1, these ePayment Conditions of Use apply to the following transactions:
- (a) 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
 - (b) telephone banking and bill payment transactions
 - (c) internet banking transactions, including 'Pay Anyone'
 - (d) online transactions performed using a card number and expiry date
 - (e) online bill payments (including BPAY®)
 - (f) direct debits
 - (g) transactions using mobile devices

Section 4. WHEN YOU ARE NOT LIABLE FOR LOSS

- 4.1. You are not liable for loss arising from an unauthorised transaction if the cause of the loss is any of the following:
- (a) fraud or negligence by our employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent
 - (b) a device, identifier or pass code which is forged, faulty, expired or cancelled
 - (c) a transaction requiring the use of a device and/or pass code that occurred before the user received the device and/or pass code (including a reissued device and/or pass code)
 - (d) a transaction being incorrectly debited more than once to the same facility
 - (e) an unauthorised transaction performed after we have been informed that a device has been misused, lost or stolen, or the security of a pass code has been breached.
- 4.2. You are not liable for loss arising from an unauthorised transaction that can be made using an identifier without a pass code or device. Where a transaction can be made using a device, or a device and an identifier, but does not require a pass code, you are liable only if the user unreasonably delays reporting the loss or theft of the device.
- 4.3. You are not liable for loss arising from an unauthorised transaction where it is clear that a user has not contributed to the loss.
- 4.4. In a dispute about whether a user received a device or pass code:
- (a) there is a presumption that the user did not receive it, unless we can prove that the user did receive it
 - (b) we can prove that a user received a device or pass code by obtaining an acknowledgement of receipt from the user
 - (c) we may not rely on proof of delivery to a user's correct mailing or electronic address as proof that the user received the device or pass code.

Section 5. WHEN YOU ARE LIABLE FOR LOSS

- 5.1. If Section 4 does not apply, you may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this Section 5.
- 5.2. Where we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the pass code security requirements in Section 6:
- (a) you are liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of pass code security is reported to us
 - (b) you are not liable for the portion of losses:
 - (i) incurred on any one day that exceeds any applicable daily transaction limit
 - (ii) incurred in any period that exceeds any applicable periodic transaction limit
 - (iii) that exceeds the balance on the facility, including any pre-arranged credit
 - (iv) incurred on any facility that we and you had not agreed could be accessed using the device or identifier and/or pass code used to perform the transaction.
- 5.3. Where:

- (a) more than one pass code is required to perform a transaction; and
- (b) we prove that a user breached the pass code security requirements in Section 6 for one or more of the required pass codes, but not all of the required pass codes

you are liable under clause 5.2 only if we also prove on the balance of probability that the breach of the pass code security requirements under Section 6 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

- 5.4. You are liable for losses arising from unauthorised transactions that occur because a user contributed to losses by leaving a card in an ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.

Note: Reasonable safety standards that mitigate the risk of a card being left in an ATM include ATMs that capture cards that are not removed after a reasonable time and ATMs that require a user to swipe and then remove a card in order to commence a transaction.

- 5.5. Where we can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a device, or that the security of all pass codes has been breached, you:

- (a) are liable for the actual losses that occur between:
 - (i) when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and
 - (ii) when the security compromise was reported to us
- (b) are not liable for any portion of the losses:
 - (i) incurred on any one day that exceeds any applicable daily transaction limit
 - (ii) incurred in any period that exceeds any applicable periodic transaction limit
 - (iii) that exceeds the balance on the facility, including any pre-arranged credit
 - (iv) incurred on any facility that we and you had not agreed could be accessed using the device and/or pass code used to perform the transaction.

Note: You may be liable under clause 5.5 if you were the user who contributed to the loss, or if a different user contributed to the loss.

- 5.6. Where a pass code was required to perform an unauthorised transaction, and clauses 5.2-5.5 do not apply, you are liable for the least of:

- (a) \$150, or a lower figure determined by us
- (b) the balance of the facility or facilities which we and you have agreed can be accessed using the device and/or pass code, including any prearranged credit
- (c) the actual loss at the time that the misuse, loss or theft of a device or breach of pass code security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.

- 5.7. In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under clauses 5.2 and 5.5:

- (a) we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring
- (b) the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in Section 6
- (c) the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example, the number and expiry date of a device) is not relevant to a user's liability.

- 5.8. If a user reports an unauthorised transaction on a credit card account, debit card account or charge card account we will not hold you liable for losses under Section 5 for an amount greater than your liability if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights).

This clause does not require us to exercise any rights we may have under the rules of the card scheme. However, we cannot hold you liable under this clause for a greater amount than would apply if we had exercised those rights.

Section 6. PASS CODE SECURITY REQUIREMENTS

- 6.1. Section 6 applies where one or more pass codes are needed to perform a transaction.
- 6.2. A user must not:
- (a) voluntarily disclose one or more pass codes to anyone, including a family member or friend
 - (b) where a device is also needed to perform a transaction, write or record pass code(s) on a device, or keep a record of the pass code(s) on anything:
 - (i) carried with a device
 - (ii) liable to loss or theft simultaneously with a deviceunless the user makes a reasonable attempt to protect the security of the pass code
 - (c) where a device is not needed to perform a transaction, keep a written record of all pass codes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the pass code(s).
- 6.3. For the purpose of clauses 6.2(b)–6.2(c), a reasonable attempt to protect the security of a pass code record includes making any reasonable attempt to disguise the pass code within the record, or prevent unauthorised access to the pass code record, including by:
- (a) hiding or disguising the pass code record among other records
 - (b) hiding or disguising the pass code record in a place where a pass code record would not be expected to be found
 - (c) keeping a record of the pass code record in a securely locked container
 - (d) preventing unauthorised access to an electronically stored record of the pass code record.
- This list is not exhaustive.
- 6.4. A user must not act with extreme carelessness in failing to protect the security of all pass codes where extreme carelessness means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour.
- Note 1: An example of extreme carelessness is storing a user name and pass code for internet banking in a diary, or mobile phone or computer that is not password protected, under the heading 'Internet banking codes'.*
- Note 2: For the obligations applying to the selection of a pass code by a user, see clause 6.5.*
- 6.5. A user must not select a numeric pass code that represents their birth date, or an alphabetical pass code that is a recognisable part of their name, if we have:
- (a) specifically instructed the user not to do so
 - (b) warned the user of the consequences of doing so.
- 6.6. The onus is on us to prove, on the balance of probability, that we have complied with clause 6.5.
- 6.7. Where we expressly authorise particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the pass code security requirements in Section 6.
- 6.8. Where we expressly or implicitly promote, endorse or authorise the use of a service for accessing a facility (for example, by hosting an access service on our electronic address), a user who discloses, records or stores a pass code that is required or recommended for the purpose of using the service does not breach the pass code security requirements in Section 6

Section 7. LIABILITY FOR LOSS CAUSED BY SYSTEM OR EQUIPMENT MALFUNCTION

- 7.1. You are not liable for loss caused by the failure of a system or equipment provided by any party to a shared electronic network to complete a transaction accepted by the system or equipment in accordance with a user's instructions.

- 7.2. Where a user should reasonably have been aware that a system or equipment provided by any party to a shared electronic network was unavailable or malfunctioning, our liability is limited to:
- (a) correcting any errors;
 - (b) refunding any fees or charges imposed on the user.

Section 8. NETWORK ARRANGEMENTS

- 8.1. We must not avoid any obligation owed to you on the basis that:
- (a) we are a party to a shared electronic payments network;
 - (b) another party to the network caused the failure to meet the obligation.
- 8.2. We must not require you to:
- (a) raise a complaint or dispute about the processing of a transaction with any other party to a shared electronic payments network
 - (b) have a complaint or dispute investigated by any other party to a shared electronic payments network.

Section 9. MISTAKEN INTERNET PAYMENTS

- 9.1. In this Section 9:
- (a) **direct entry** means a direct debit or direct credit
 - (b) **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:
 - (i) the user's error, or
 - (ii) the user being advised of the wrong BSB number and/or identifier.
 This does not include payments made using BPAY®.
 - (c) **receiving ADI** means an ADI whose customer has received an internet payment
 - (d) **unintended recipient** means the recipient of funds as a result of a mistaken internet payment
- 9.2. When you report a mistaken internet payment, we must investigate whether a mistaken internet payment has occurred.
- 9.3. 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.*
- 9.4. If we are not satisfied that a mistaken internet payment has occurred, we will not take any further action.
- 9.5. 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.
- 9.6. You may complain to us about how the report is dealt with, including that we and/or the receiving ADI:
- (a) are not satisfied that a mistaken internet payment has occurred
 - (b) have not complied with the processes and timeframes set out in clauses 9.2-9.5, or as described in the box below.
- 9.7. When we receive a complaint under clause 9.6 we must:
- (a) deal with the complaint under our internal dispute resolution procedures
 - (b) not require you to complain to the receiving ADI.
- 9.8. 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.

- 9.9. If you receive a mistaken internet payment into your account and we are required under the ePayments Code as receiving ADI to return the funds to the payer's ADI then we will, without seeking your consent, transfer the funds from your account. If there are insufficient funds in your account you must co-operate with us to facilitate repayment of the funds.

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 TELEPHONE, INTERNET OR MOBILE BANKING

10.1. We do not warrant that:

- (a) the information available to you about your accounts through our telephone, internet or mobile banking service is always up to date;
- (b) you will have 24 hours a day, 7 days per week, access to telephone, internet or mobile banking;
- (c) data you transmit via telephone, internet or mobile banking is totally secure.

Section 11. HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR ACCESS CARD OR PASS CODE

11.1. If you believe your access card has been misused, lost or stolen or the pass code has become known to someone else, you must immediately contact us during business hours or the access card HOTLINE at any time.

Please refer to How to Contact Us on page 2 for our contact details.

11.2. 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.

11.3. The access card HOTLINE is available 24 hours a day, 7 days a week.

11.4. If the 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 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.

11.5. 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:

- (a) with us by telephone or priority paid mail as soon as possible; or
- (b) by telephoning the VISA Card Hotline number for the country you are in.

VISA CARD HOTLINE AUSTRALIA WIDE TOLL FREE 1800 621 199 FROM OVERSEAS +61 2 9959 7480	CUECARD HOTLINE AUSTRALIA WIDE TOLL FREE 1800 621 199 FROM OVERSEAS +61 2 9959 7480
--	--

Section 12. HOW TO REPORT UNAUTHORISED USE OF TELEPHONE, INTERNET OR MOBILE BANKING

12.1. If you believe that your pass codes for telephone, internet or mobile banking transactions have 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 2 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.

12.2. If you believe an unauthorised transaction has been made and your access method uses a pass code, you should change that pass code.

Section 13. USING THE ACCESS CARD

13.1. You agree to sign the access card immediately upon receiving it and before using it as a means of preventing fraudulent or unauthorised use of access card. You must ensure that any other

cardholder you authorise also signs their access card immediately upon receiving it and before using it.

13.2. We will advise you from time to time:

- (a) what transactions may be performed using access card;
- (b) what ATMs of other financial institutions may be used; and
- (c) what the daily cash withdrawal limits are.

Please refer to Interest, Fees and Charges brochure for details of current transaction limits

13.3. You may only use your access card to perform transactions on those accounts we permit. We will advise you of the accounts which you may use your access card to access.

13.4. The access card always remains our property.

Section 14. USING VISA OR CUECARD OUTSIDE AUSTRALIA

14.1. All transactions made in a foreign currency on the 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).

14.2. All transactions made in a foreign currency [or with a merchant located overseas (even if in Australian currency)] on the Visa Card or CueCard are subject to a conversion fee. Please refer to the *Interest, Fees and Charges* brochure for the current conversion fee.

14.3. Some overseas Merchants and electronic terminals charge a surcharge for making a 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.

14.4. Some overseas Merchants and electronic terminals allow the cardholder the option to convert the value of the Transaction into Australian dollars at the point of sale, also known as Dynamic Currency Conversion. Once you have confirmed the transaction you will not be able to dispute the exchange rate applied.

Section 15. ADDITIONAL ACCESS CARD

15.1. You may authorise us, if we agree, to issue an additional access card to an additional cardholder provided this person is over the age of 18 (unless we agree to a younger age).

15.2. You will be liable for all transactions carried out by this cardholder.

15.3. We will give each additional cardholder a separate pass code.

15.4. You must ensure that any additional cardholders protect their access card and pass code in the same way as these ePayment Conditions of Use require you to protect access card and pass code.

15.5. To cancel the additional access card you must notify us by telephone, in person at any branch or in writing (including electronically).

Please refer to How To Contact Us on page 2 for our contact details.

15.6. You will not be liable for the continued use of the additional access card after its cancellation.

Section 16. USE AFTER CANCELLATION OR EXPIRY OF ACCESS CARD

16.1. You must not use your access card:

- (a) before the valid date or after the expiration date shown on the face of access card; or
- (b) after the access card has been cancelled.

16.2. 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 17. EXCLUSIONS OF ACCESS CARD WARRANTIES AND REPRESENTATIONS

- 17.1. We do not warrant that Merchants or ATMs displaying access card signs or promotional material will accept access card.
- 17.2. We do not accept any responsibility should a merchant, bank or other institution displaying access card signs or promotional material, refuse to accept or honour access card.
- 17.3. 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 18. CANCELLATION OF ACCESS CARD OR OF ACCESS TO TELEPHONE, INTERNET OR MOBILE BANKING, BPAY®

- 18.1. You may cancel your access card, your access to telephone, internet or mobile banking or BPAY® at any time by giving us written notice.
- 18.2. We may immediately cancel or suspend your access card or your access to telephone, internet or mobile banking, BPAY® at any time:
 - (a) for security reasons,
 - (b) if you breach these Conditions of Use
 - (c) you, or someone acting on your behalf, is being fraudulent
 - (d) for any other reason set out in Closing Accounts, Cancelling Access Facilities & Blocking Access or Transactions on page 10.

In the case of access card, we may cancel the access card by capture of the access card at any ATM.

- 18.3. We may cancel your access card or your access to telephone, internet or mobile banking, BPAY® for any reason by giving you 30 days' notice. The notice does not have to specify the reasons for cancellation.
- 18.4. In the case of access card, you will be liable for any transactions you make using your access card before the access card is cancelled but which are not posted to your account until after cancellation of access card.
- 18.5. In the case of telephone, internet or mobile banking, or BPAY®, if, despite the cancellation of your access to the relevant access method, you carry out a transaction using the relevant access method, you will remain liable for that transaction.
- 18.6. Your access card or your access to telephone, internet or mobile banking, or BPAY® will be terminated when:
 - (a) we notify you that we have cancelled your access card or your access method to the account with us;
 - (b) you close the last of your accounts with us to which the access card applies or which has telephone, internet or mobile banking, or BPAY® access;
 - (c) you alter the authorities governing the use of your account or accounts to which the access card applies or which has telephone, internet or mobile banking, or BPAY® access (unless we agree otherwise).
- 18.7. In the case of access card, we may demand the return or destruction of any cancelled access card.

Section 19. USING BPAY®

- 19.1. You can use BPAY® to pay bills bearing the BPAY® logo from those accounts that have the BPAY® facility.
- 19.2. 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.
- 19.3. We cannot effect your BPAY® instructions if you do not give us all the specified information or if you give us inaccurate information.

Please note that, legally, the receipt by a biller of a mistaken or erroneous payment does not necessarily discharge, wholly or in part, the underlying debt you owe that biller.

Section 20. PROCESSING BPAY® PAYMENTS

- 20.1. We will attempt to make sure that your BPAY® payments are processed promptly by participants in BPAY®, and you must tell us promptly if:
- (a) you become aware of any delays or mistakes in processing your BPAY® payment;
 - (b) you did not authorise a BPAY® payment that has been made from your account; or
 - (c) 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.*
- 20.2. A BPAY® payment instruction is irrevocable.
- 20.3. Except for future-dated payments you cannot stop a BPAY® payment once you have instructed us to make it and we cannot reverse it.
- 20.4. We will treat your BPAY® payment instruction as valid if, when you give it to us, you use the correct access method.
- 20.5. 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).
- 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.*
- 20.6. A BPAY® payment is treated as received by the biller to whom it is directed:
- (a) 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
 - (b) otherwise, on the next banking business day after you direct us to make it.
 - (c) 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.
- 20.7. Notwithstanding this, a delay may occur processing a BPAY® payment if:
- (a) there is a public or bank holiday on the day after you instruct us to make the BPAY® payment;
 - (b) 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
 - (c) a biller, or another financial institution participating in BPAY®, does not comply with its BPAY® obligations.
- 20.8. If we are advised that your payment cannot be processed by a biller, we will:
- (a) advise you of this;
 - (b) credit your account with the amount of the BPAY® payment; and
 - (c) take all reasonable steps to assist you in making the BPAY® payment as quickly as possible.
- 20.9. 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:
- (a) 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
 - (b) 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.
- 20.10. 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 21. FUTURE-DATED BPAY® PAYMENTS

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

You may arrange BPAY® payments up to 60 days in advance of the time for payment. 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 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;
- (b) 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;
- (c) you are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly;
- (d) you should contact us if there are any problems with your future-dated payment;
- (e) 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 22. CONSEQUENTIAL DAMAGE FOR BPAY® PAYMENTS

- 22.1. 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.
- 22.2. We are not liable for any consequential loss or damage you suffer as a result of using BPAY®, 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.

COMPLAINTS

If you want to make a complaint, please speak to our staff:

- at any branch; or
- by calling 08 8999 0777.

You may also make a complaint:

- by emailing info@tcu.com.au;
- by fax 08 8999 0788;
- by completing a “TCU Member Compliant Form” at <https://tcu.com.au/help/complaints-and-feedback/>; or
- by writing to TCU COMPLAINTS, PO BOX 40425, CASUARINA, NT 0811.

We will handle your complaint fairly and try to resolve it as soon as possible. If we cannot resolve the issue on the spot, we will do our best to complete our investigation and inform you of our decision within 21 days. We will let you know if we need more time.

For more information about our complaint handling process we have a guide to our dispute resolution system available on our website or on request.

Australian Financial Complaints Authority

If you are not satisfied with our response, or handling of your complaint, you may refer the matter to the Australian Financial Complaints Authority (AFCA). AFCA provides a free and independent external resolution service. You can contact AFCA at:

Postal Address: Australian Financial Complaints Authority Limited
GPO Box 3
Melbourne VIC 3001

Website: www.afca.org.au

Email: info@afca.org.au

Telephone: 1800 931 678

Customer Owned Banking Code of Practice compliance

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice, you can contact the Customer Owned Banking Code Compliance Committee. Please be aware that the Committee is not a dispute resolution body and cannot provide financial compensation. You can contact the Committee at:

Postal Address: Customer Owned Banking Code Compliance Committee
PO Box 14240
Melbourne VIC 8001

Website: www.cobccc.org.au

Email: info@codecompliance.org.au

Telephone: 1800 931 678

VERIFIED BY VISA

Where there is any inconsistency between the EFT Access Facilities and EFT Conditions of Use or Visa Card conditions of use found in this document, the EFT Access Facilities and EFT Conditions of Use or Visa Card conditions will apply to the extent of the inconsistency. Each time you complete or attempt to complete a Verified by Visa (VBV) transaction, you are deemed to accept these conditions.

USING THE VBV VISA SERVICE

You may use VBV to make purchases online. However, the VBV service may only be available in connection with participating online merchants. When making an online purchase or other transaction for which VBV 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. The information that you provide may be validated against information we hold about you and may be validated against information held by third parties.

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.

A Third Party Operator may use the VBV service if they hold a Visa Card linked to your Account. The Third Party Operator will be asked to provide information to us that allows us to validate the identity and verify that they are the cardholder of the specified Visa Card. The information that they provide may be validated against information we hold about them and maybe validated against information held by third parties.

PRIVACY

We (or our nominated service provider) may collect personal information about you for the purposes of providing the VBV service to you. You authorise us to disclose personal information to others in order to execute your instructions including, but not limited to, conducting the VBV service and investigating disputes or allegations of unauthorised transactions, or if it is required by law. For more details of how your personal information is handled, please refer to our privacy policy, which can be viewed by accessing www.tcu.com.au

TERMINATION OF VERIFIED BY VISA

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

PARTICIPATING ONLINE MERCHANTS

You will know that an online merchant is a participating online merchant because you will see the VBV logo and you may be asked to verify your identity before completing an online transaction with that merchant.

We do not endorse or recommend in any way any participating online merchant. Your correspondence or business dealings with, or participation in promotions of, online stores through VBV, including payment for and delivery of related goods or services not purchased via VBV, 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.

EXCLUSION OF LIABILITIES

Subject to any warranty which is imported into these conditions by law and which cannot be excluded, the VBV 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.

We will not be liable for any damages whatsoever arising out of or in relation to:

- your use of or access to (or inability to use or access) the VBV services; or
- any other failure of performance, error, omission, interruption or defect, or any loss or delay in transmission or a transaction.

If you are dissatisfied with any aspect of the VBV service, your sole and exclusive remedy is to terminate participation in the VBV transaction or service, as provided in these conditions.

YOUR CONDUCT

Whilst using the VBV service and Traditional Credit Union’s Internet Banking services, you agree not to:

1. impersonate any person or entity using the VBV authentication process;
2. 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 VBV service or by us;
3. spam or flood our Internet Banking service and the VBV service;
4. modify, adapt, sub-license, translate, sell, reverse engineer, decompile or disassemble any portion of the VBV service.
5. remove any copyright, trademark, or other proprietary rights notices contained in the VBV service;
6. “frame” or “mirror” any part of the VBV service without our prior written authorisation;
7. 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 VBV service;
8. otherwise interfere with, or disrupt the VBV service or our Internet Banking services or servers or networks connected to us or the VBV service or violate these conditions or any requirements, procedures, policies or regulations in relation to the VBV service; or
9. intentionally or unintentionally violate any applicable local, state, national or international laws or regulations relevant or applicable to the VBV service.

YOUR LIABILITY

Your liability for unauthorised transactions is governed by the EFT Access Facilities and EFT Conditions of Use (above). If you breach these conditions, this may affect your liability for unauthorised transactions. If it is determined that you have contributed to the loss, you may be held liable for the transactions notwithstanding that they are unauthorised.

ERRORS

If you believe a VBV transaction is wrong or unauthorised or a periodical statement contains any instances of unauthorised use or errors, you should contact us immediately.

SUMMARY OF ACCOUNTS & AVAILABILITY OF ACCESS FACILITIES

TRANSACTIONAL AND SAVINGS ACCOUNTS**Everyday Account (S1)**

This is an everyday transaction and savings account which you can use for your day to day banking. This Account gives you full access to all of our Branches, Call Centre, ATMs and Digital channels and as you balance builds it pays higher interest.

Budget Account (S2)

This account enables you to have separate accounts for different purposes. You may want to put money aside for bills or to save for a specific item. If you maintain a balance of \$250 or more for the whole month the Account Fee is reduced to Nil.

Christmas Club Account (S3)

This account that can be used for saving money throughout the year. You then use this money for Christmas presents, holidays or other special occasions.

Family / Clan / Group Account (S4)

This account that can be used by a whole family, clan or group (Sporting Club, etc). It can be set up so that multiple signatures are required to access the money in this account. This account is useful for families or clan groups who receive money or income such as royalties that are paid to the whole family rather than an individual.

Student Account (S6)

Transaction Account designed for students aged between 13 and 18 years.

TCU Online Account (S10)

This account is an everyday low fee transaction account...You can access it via Internet and Mobile Banking, EFTPoS or ATMs. Branch use is available in emergencies but may incur extra fees.

If your account goes overdrawn, any fees or interest charged will be refunded within 30 days.

Child Account (S9)

This account is designed for children from birth to age 12. This account can be opened by a parent or guardian on behalf of a minor. Both the child and the parent or guardian must provide identification on opening of the account.

Accounts opened for Minors under the age of 13 (at time of Account opening):

- the Child Account (S9) can be opened in the name of a Minor under the age of 13. A minor under the age of 13 cannot be an Account holder (solely or jointly) of any other Account types;
- a Child Account (S9) can be opened by a parent(s), legal guardian(s) or other adult(s) on behalf of the Minor;
- the person(s) who opens a Child Account (S9) must be a Third Party Operator(s) when the Account is opened and may operate the Account in that capacity subject to the terms of the Account operating authority, the Minor may only operate a Savings Account (while a Minor) with the express, written consent of the Third Party Operator(s) given in a form we approve and in accordance with the Account operating authority. The Minor may then operate the Account in accordance with the Account operating authority (as varied to include the Minor). Minors under the age of 10 years cannot be authorised to operate the Account;
- a Minor who has been given authority to operate a Savings Account can, if the Account operating authority specifies 'only one to sign', unilaterally change the Account operating authority, appoint a Third Party Operator(s) and/or remove any Third Party Operator's authority to operate the Account;

- we do not recommend the provision of Card, Phone Banking or Internet Banking access to Minors under the age of 13. However, Card (CueCard only for Minors under 16), Phone Banking and Internet Banking access may be provided to a Minor aged 10 years or older with the express consent of the Third Party Operator(s) given in accordance with an Account operating authority and where the Account type permits these access facilities.
- On opening a child account both the child and the signatory must provide proof of identity.

Accounts opened for or by Minors aged 13 years and over (at time of Account opening):

- a Student Account may be opened by a parent(s), legal guardian(s) or other adult(s) on behalf of the Minor.
- a Student Account may be opened by a Minor independently and without permission from any parent, legal guardian or other adult.
- subject to the other terms and conditions applying to the Account, a Minor will have unrestricted rights to operate the Account if the Account is in the Minor's sole name and in accordance with the Account operating authority in the case of a Joint Account;
- a Minor may authorise, unilaterally if the Account is in the Minor's sole name or in accordance with the Account operating authority in the case of a Joint Account, one or more Third Party Operators to operate the Account in writing in a form we approve. A Minor may, unilaterally if the Account is in the Minor's sole name or in accordance with the Account operating authority in the case of a Joint Account, change the Account operating authority and/or remove any Third Party Operator's authority to operate the Account;
- Card (CueCard only for Minors under 16 years), Phone Banking and Internet Banking Account access by the Minor will be permitted where the Account type permits these access facilities.

We will only open an Account at the independent request of a Minor, or grant access to a Minor to a Student Account at the request of a Third Party Operator(s), where the Minor is able to register a consistent specimen signature to our satisfaction.

We reserve the right to decline to open an Account for a Minor, or grant access to an Account to a Minor at the request of a Third Party Operator(s), if we consider it reasonably necessary to decline in order to protect our interests, those of an Accountholder or those of a Minor.

We reserve the right to remove a Third Party Operator, restrict the ability of a Third Party Operator to operate on the Account of a Minor or otherwise change the Account operating authority of the Account of a Minor where we consider it reasonably necessary to do so in order to protect our interests, those of an Accountholder or those of a Minor.

In relation to an Account with a Minor Account holder, each joint Account holder who isn't a Minor and each Third Party Operator on the Account agrees to indemnify us and keep us indemnified against all claims (including any claim made by the Minor), obligations, liabilities, expenses, losses, damages and costs that we may sustain or incur as a result of any transaction carried out on the Account while they are a joint Accountholder who isn't a Minor or Third Party Operator (even if they are no longer a joint Accountholder or Third Party Operator at the time indemnity is sought) by:

- them;
- a minor;
- any joint Accountholder; and/or
- any Third-Party Operator on the Account.

The above-mentioned indemnity does not require a joint Account holder or Third Party Operator to indemnify us for any claims, obligations, liabilities, expenses, losses, damages or costs to the extent they arise from any fraud, negligence or wilful misconduct by us or our officers, employees, contractors or agents.

For the avoidance of doubt, any credit balance in a Minor's Account is at all times the property of the Minor in the case of an Account in the sole name of a Minor and is the joint property of all the Account holders (including each Minor) in the case of a Joint Account.

Where the Account operating authority stipulates "only one to sign", Card access may be provided to a Third Party Operator where the Account type permits Card access.

[illegible]

INVESTMENTS (TERM DEPOSITS)

Term Deposits are used to put your money aside and to earn you interest on your money. If you receive a special payment, such as a tax return, Centrelink bonus, or royalty payment, you can put some or all of that money into a Term Deposit to help it last longer and earn interest.. Term Deposits can be opened at any TCU branch. Terms range from 30 days to 2 years. Interest is calculated daily and paid on maturity. Interest may be paid directly to an account or compounded and added to the Term Deposit. Funds are fixed and cannot be withdrawn until the term expires.

On maturity of your term investment account, TCU will notify you of the maturity details. In accordance with ASIC Corporations (TD Rollovers) Instrument 2025/172, TCU may issue a combined maturity notice, or separate pre- and post-maturity notices, depending on operational processes. A combined notice will be provided at least five business days and no more than 10 business days before maturity and will include an indicative interest rate that would apply to a new term deposit if rolled over. You must advise us of your instructions for the funds before the end of the Grace Period following maturity. TCU will take reasonable steps to meet all applicable notice timeframes. Refer to Interest, Fees and Charges brochure for more information.

BUSINESS ACCOUNTS

We offer a range of Business Accounts that will suit most business's needs. You can open multiple business accounts and sub accounts if you need to manage multiple budgets. You can pay bills, access business Internet Banking and process payrolls from our Business Accounts.

ACCOUNT TYPE	LOW USAGE PLAN (S24)	MEDIUM USAGE PLAN (S25)	HIGH USAGE PLAN (S26)	BENEVOLENT ACCOUNT (S28)
Eligibility	Business, Shires, & Companies	Business, Shires, & Companies	Business, Shires, & Companies	Not for profit – Charities
Minimum Opening Balance	Nil	Nil	Nil	Nil
Minimum Ongoing Balance	Nil	Nil	Nil	Nil
Fund available at call	Yes	Yes	Yes	Yes
Minimum withdrawal amount	Nil	Nil	Nil	Nil
Branch Access	Yes	Yes	Yes	Yes
Visa Debit Card or CueCard	No	No	No	No
Purchase goods and withdraw funds using EFTPOS	No	No	No	No
BPAY	Yes	Yes	Yes	Yes
Direct Credits Allowed	Yes	Yes	Yes	Yes
Direct Debits Allowed	Yes	Yes	Yes	Yes
Internet Banking and Mobile Banking	Yes	Yes	Yes	Yes
Withdrawal Limits	Nil	Nil	Nil	Nil
Statements Sent	Bi-annually -refer note 5	Bi-annually -refer note 5	Bi-annually -refer note 5	Bi-annually -refer note 5

NOTES FOR SUMMARY OF ACCOUNTS & AVAILABILITY OF ACCESS FACILITIES

Note 1 - Our standard Internet Banking daily limits are set out in the table below.

You can ask us to increase or decrease these limits by contacting us. It is at our absolute discretion as to whether we accept or decline such a request.

We may also increase or decrease the limits that apply to you at any time at our absolute discretion without your consent. Where we are required to do so by the ePayments Code, we will notify you of such a change.

The standard Internet Banking daily limits set out in the table below will not affect any non-standard limit we have agreed or otherwise set for you.

LIMIT TYPE	LIMIT DESCRIPTION	LIMIT VALUE	MAXIMUM VALUE
BPAY Payments	All BPAY Payments	\$ 10,000	\$ 100,000
Internal Payments (member-to-member)	Transfers from your Accounts to other accounts with us, not within the same Membership.	\$ 10,000	\$ 100,000
Internal Transfers (within Membership)	All transfers between your Accounts with us (within the same Membership)	\$ 10,000	\$ 100,000
External Payments	The total of all External Transfer Payments made using a BSB and account number	\$ 10,000	\$ 100,000

Note 2 - Visa Debit Card access allowed from the age of 16 only. Upon turning 19 years of age, your *S6 Student Account* will be converted to a *S1 Savings Account* or if eligible a *S10 TCU Online Account*. Applicable fees and charges will apply to the *S1 Savings Account* or *S10 TCU Online Account* on conversion as set out in our "Interest, Fees & Charges" brochure.

Note 3 - During the withdrawal access period between 1 November and 31 December each year, free Branch/Agency withdrawals apply. Internet and Phone Banking transfers are allowed during the access period. Withdrawals are allowed outside this access period however a charge may apply. Refer to our "Interest, Fees & Charges" brochure.

Note 4 - Where an Account allows Visa facilities, ATM, EFTPOS, Internet Banking, Phone Banking and BPAY access, they are only available where the Account requires only one signature for withdrawals.

Note 5 - You may request for your statements to be sent monthly.

Note 6 - Upon turning 13 years of age, your *S9 Child Account* will be converted to a *S6 Student Account*.