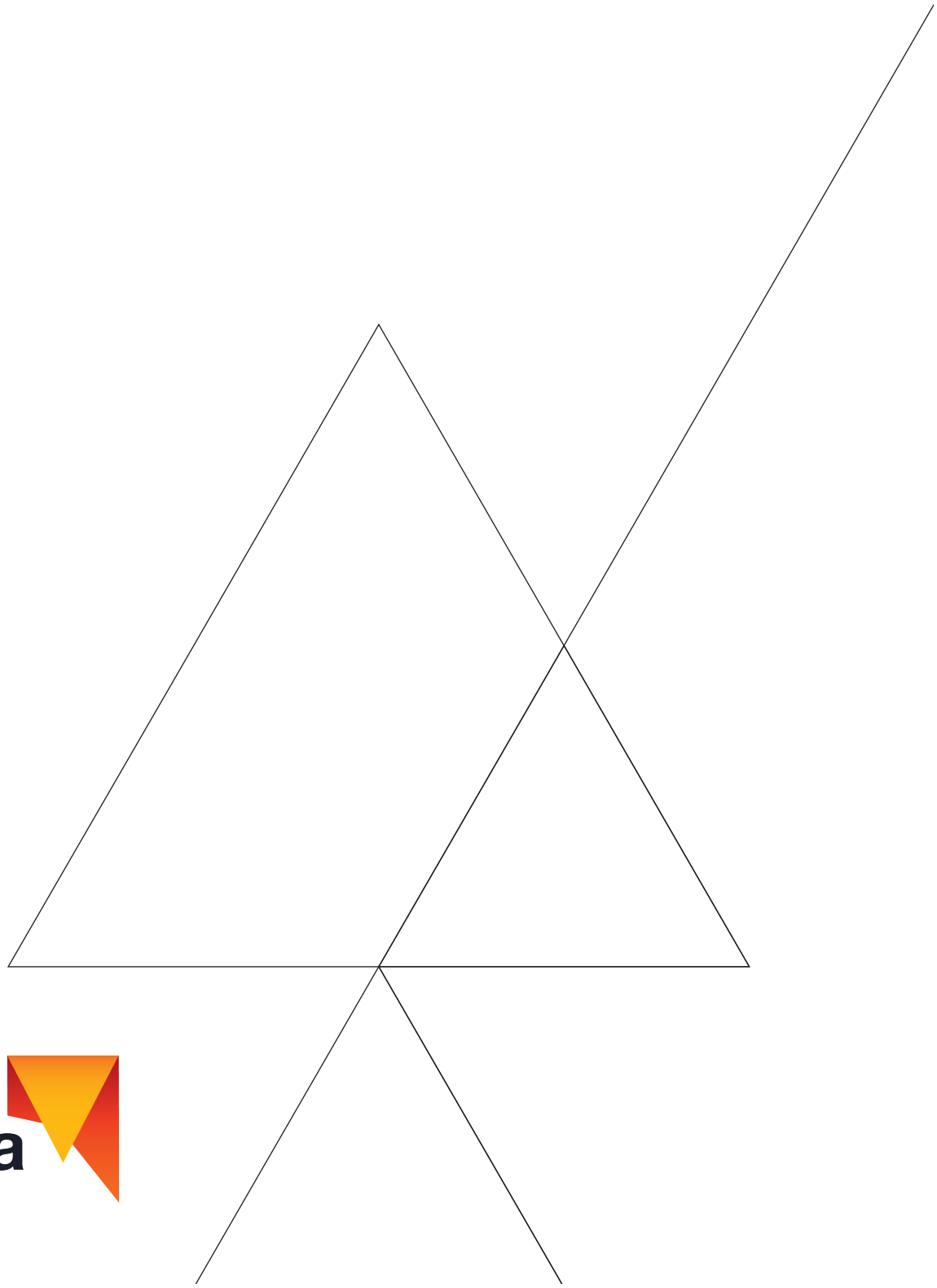
Deposit Accounts and Access Services

Terms and Conditions

Effective 29 April 2024



credit unionsa

About this document

This document and the *Deposit Accounts Fees and Charges* and the *Deposit Accounts Interest Rates* documents form the terms and conditions that apply to our deposit accounts and access services and are binding on you when you open an account or use an access service. We urge you to read all of the documents carefully.

The latest version of all documents is available at a branch or on our website creditunionsa.com.au or contact our Member Experience Centre on 08 8202 7777 (1800 018 227 for Country SA members) to be sent a copy.

Table of contents

Part 1
General information

1. Definitions

In this document, words have the following meanings:

access code is the password or number used to access your accounts via our Member Experience Centre;

access method is a method using a device we authorise for you to access your accounts to perform EFT transactions but excludes a method requiring a manual signature;

access service is a service to access an account and includes an access method;

account means a deposit account with us;

account holder means the person or persons in whose name the account is held;

ADI means an authorised deposit taking institution under the *Banking Act 1959* (Cth);

AML/CTF Act means the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth);

ASIC means the Australian Securities and Investments Commission;

ATM means an automatic teller machine;

authorised user means you and any person you have authorised to use your account;

available balance means the funds available for immediate withdrawal from an account excluding deposits received but uncleared in accordance with our policy, deposits in transit or interest accrued but not credited;

Bank@Post is a facility provided by Australia Post at its participating outlets that allows you to perform selected transactions on your accounts when linked to a card;

biller is an organisation who tells you that you can make bill payments to them through BPAY®;

BPAY means BPAY Pty Ltd ABN 69 079 137 518;

BPAY Payment is a payment transacted through BPAY to make bill payments to billers who participate in BPAY, either via telephone, internet, or any other access method;

BSB number means Bank/State/Branch number;

business day is a day that is not a Saturday, Sunday or public holiday or bank holiday in the place concerned;

card is any authorised Visa card or rediCARD issued by us for your account;

card details means the information provided on a card including the card number and expiry date;

card hotline is the facility made available to you to report of a lost or stolen card. The card hotline is 1800 648 027;

code of practice means the Customer Owned Banking Code of Practice;

Credit Reporting Code means the *Privacy (Credit Reporting) Code 2014*;

Cuscal means Cuscal Limited ABN 95 087 822 455;

cut off time is the time we tell you when your payment instructions (such as BPAY) must be received by us to be processed that day;

day means a 24-hour period commencing on midnight in the place concerned;

DDR is a direct debit request service agreement authority signed by you to debit amounts to your specified account;

destination account ***in relation to Round Up***, means a savings account with us that has been set up by you to be credited with the round up amount on eligible round up transactions;

device is any tangible object capable of initiating, receiving, storing or processing electronic information about your accounts, or performing transactions on your accounts, and includes a computer, mobile phone, tablet, card, token, contactless device or any other telecommunications or electronic equipment;

digital wallet is a host card emulation facility allowing you to register your Visa card in a near field communication (NFC) enabled device to perform payWave transactions;

EFTPOS is a point of sale electronic banking facility available at retail or wholesale outlets;

EFT transaction is an electronic funds transfer to or from your account using an access method;

eligible card means a Visa card which has the Visa Direct functionality to receive funds from another eligible card;

eligible Round Up transaction ***in relation to Round Up***, has the meaning ascribed in **clause 45.5**;

identifier is the information provided to perform a transaction, such as membership number, account number, BSB or card number;

Internet Banking is our website service allowing you to receive account information and perform certain transactions on your accounts, and includes Mobile Banking;

linked account is your account when linked to a card, and includes any overdraft or line of credit that we allow you to attach to your linked account;

linked loan means an eligible home loan that you link to one or more Home Loan Offset Accounts;

locked ***in relation to a PayID***, means a PayID which is temporarily disabled in the PayID Service;

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

member means a member of the Credit Union;

membership number is the number we allocate as the primary reference to your membership details;

merchant is a supplier of the goods or services purchased with a device;

Merchant ***in relation to PayTo***, means a merchant with which you have established, or would like to establish, a PayTo Agreement;

minor is a person under the age of 18 years;

Migrated DDR PayTo Agreements mean existing direct debit arrangements you have with Merchants and Payment Initiators in order to process payments under those arrangements via the NPP;

misdirected payment ***in relation to an NPP Payment***, is a payment credited to the wrong account because of an error in recording the PayID or your nominated account information in the PayID Service;

mistaken internet payment is a payment through a 'pay anyone' banking facility where funds are paid into the account of an unintended recipient because the sender uses the wrong identifier for the payee and the term is used in this document for auto transfers, NPP Payments and Osko Payments through Internet Banking but not BPAY and PayTo Payments;

mistaken payment ***in relation to an NPP Payment***, is a payment made by a payer which is credited to the wrong account because of the payer's error (except a payment made using the PayTo service);

Mobile Banking is the Internet Banking service we provide through applications, software or websites allowing you to receive information about your accounts and perform certain types of transactions on your accounts using a mobile device;

Mobile Banking App means the applications that we make available to you to access Mobile Banking from a compatible device;

not for profit organisation is an organisation that is not operating for the profit or gain of its individual members, whether direct, indirect, immediate or deferred;

NPP is the New Payments Platform operated by NPP Australia Limited ABN 68 601 428 737;

NPP International Payment means a payment you receive from overseas that will be routed through the (domestic) NPP;

NPP Payment is a payment cleared and settled via the NPP and includes an Osko Payment;

origin account ***in relation to Round Up***, means a savings account with us selected by you and set up in Round Up, as the account from which eligible Round Up transactions will be made;

Osko is the Osko Payment service provided by BPAY;

Osko Payment is a payment made by or on behalf of a payer to a payee using Osko;

Osko Scheme is the scheme operated by BPAY which governs the way in which we provide Osko to you;

overdraft limit is the limit of credit on any overdraft facility we grant to you;

passcode is a PIN, access code, Phone Banking password, Internet Banking password, Mobile Banking password, user ID, phone lock passcode, fingerprint login or any other similar information to authenticate a transaction or user, and which you are required to keep secret. A passcode may consist of numbers, letters, a combination of both, or a phrase, but does not include a number printed on a device (e.g. a security number printed on a card);

PayID is the identifier you choose to receive NPP Payments;

PayID Name is 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 Record is a combination of your PayID, PayID Name and account details (including full legal account name) in the PayID service and any other information required by NPP Australia from time to time;

PayID Service is the central payment addressing service for addressing NPP Payments;

PayID Type is the type of identifier we allow for you to select for receiving NPP Payments;

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

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

payment sender is a person who performs a transaction using a 'pay anyone' banking facility;

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

payWave is the functionality on a Visa card or enabled mobile device allowing you to make small value payments at participating merchants by waving, tapping or otherwise placing the card or device near a payWave reader;

Phone Banking is the automated telephone service we provide that lets you receive information about your accounts and perform certain types of transactions on your accounts, but excludes assistance from our Member Experience Centre;

PIN is a personal identification number or word used in conjunction with a card or Mobile Banking App when giving an instruction through electronic equipment;

Privacy Act means the *Privacy* Act *1988* (Cth).

receiving ADI is an ADI whose customer has received an internet payment;

rediCARD means the rediCARD issued to you by us. From 16 October 2023, rediCARDs will not be available to new members;

restricted transaction or function is a type of transaction or function that you can perform via Internet Banking that must be validated using a secure one-time code;

Round Up is the functionality we provide that allows you to round your eligible Round Up transactions up by an agreed amount;

secure one-time code is a unique 6-digit passcode provided by our Secure SMS or VIP Security services that provides an additional level of security when conducting certain Internet Banking restricted transactions or functions;

sending ADI is an ADI whose customer has made an internet payment;

supplier is a supplier of goods or services authorised by you to deduct payments from your account through the direct debit service;

TFN means your tax file number;

Travelex is the supplier of foreign currency. Travelex Limited ABN 36 004 179 953 AFSL 222444 (Travelex)

unauthorised transaction means a transaction that is not authorised and performed by you. It does not include any transaction that is performed by you or any authorised user, or by anyone who performs a transaction with your knowledge and consent;

unintended recipient is the recipient of funds as a result of a mistaken internet payment;

Visa card means the Visa debit card issued to you by us;

we, us, our, ours or the Credit Union means Credit Union SA Ltd ABN 36 087 651 232; and **you** means the account holder and any person authorised by you to operate the account or an access service.

Unless the context implies otherwise, a singular word includes the plural and vice versa.

2. Customer Owned Banking Code of Practice

We are bound by the Customer Owned Banking Code of Practice. Credit unions, mutual banks and mutual building societies are customer-owned financial institutions committed to putting their members first. This code of practice expresses the value we place on improving financial wellbeing of our members and communities.

This code of practice expresses our 7 key promises to you:

- We will deliver banking services in the interests of our customers.
- We will obey the law.
- We will not mislead or deceive.
- We will act honestly and fairly.
- We will offer products and services that are fit for general purpose.
- We will deliver services with reasonable care and skill.
- We will contribute to our community.

You can access a copy of the code of practice from: creditunionsa.com.au/about-us/our-ethics

3. ePayments Code

The ePayments Code applies to electronic transactions on your account that are initiated through an access method. We will comply with the ePayments Code where the code applies to your dealings with us.

4. Privacy Act

In handling your personal information, we are bound by the Australian Privacy Principles under the Privacy Act, Credit Reporting Code and the code of practice. We have a general duty of confidentiality towards you except where the disclosure is made with your consent or permitted by law.

Our Privacy Policy and Privacy Permission explains our obligation to protect and manage your personal information, including your credit related information such as your credit liabilities, repayments and defaults, and how you may complain about a breach of the Privacy Act or the Credit Reporting Code and the process by which we will handle your complaint.

Our Privacy Policy and Privacy Permission are on our website creditunionsa.com.au/legal/privacy or call the Member Experience Centre.

As outlined in our Privacy Policy we may disclose your personal information (including credit-related information) to other organisations, that provide services that assist us in supplying or administering the products and services that we offer. In accordance with our Privacy Policy we, and those organisations assisting us, may use information and data we hold in order to detect, investigate and prevent suspicious, illegal, unauthorised or fraudulent activities and comply with our legislative and regulatory obligations.

5. Financial Claims Scheme

The Australian Government's Financial Claims Scheme protects depositors by providing a guarantee on deposits up to $250,000 held with ADIs and allows them access to their deposits if an ADI becomes insolvent. We are an ADI.

You can get information about the scheme at ***www.fcs.gov.au*** or calling 1300 558 849.

6. Financial difficulty

If you are in financial difficulty you should contact us immediately. We are here to serve our members, and the earlier you let us know that you are experiencing financial difficulties, the sooner we may be able to assist you.

7. Feedback

We encourage regular, honest feedback from our members. So please don't hesitate to contact us.

8. Changes to these terms and conditions

Refer to **clause 34**.

9. Complaints and resolving disputes

Refer to **Part 6**.

Part 2
How to open an account

10. Become a member

You need to become a member of Credit Union SA before we will open an account for you, and you cannot have an access service without an account. To become a member, you need to complete a membership application at a branch or by contacting our Member Experience Centre or via our website ***www.creditunionsa.com.au***

If we accept your application, you become a shareholding member (the share costs nothing $0) and you are bound by our Constitution. Our constitution is on our website ***www.creditunionsa.com.au***

Memberships and accounts can be opened for individuals and for business use (such as companies, trusts, clubs and societies).

11. What accounts can you open?

When we open your membership, you will be given an Access Account. You can open other accounts as needed.

Clause 19 contains a **Table** summarising the account types, some conditions applying to them and the access methods available.

12. Identifying and verifying your identity

Before opening or allowing access to an account we must confirm your identity, and that of any joint account holders and authorised users as required by the AML/CTF Act and our identification policy. We may obtain additional information from you such as the source of funds in your account or how you plan to use your account. We may use a third-party provider to verify some or all of this information.

For business accounts, we need to collect and verify additional information about the entity and may collect and verify personal information about any persons who hold a beneficial or controlling interest in the entity.

By opening an account with us, you agree that all details you provide to us are true and correct. It may be an offence if you deliberately provide us with incorrect or false information.

The law may require us to disclose information regarding your banking transactions to regulators and law enforcement agencies. The law may prohibit us from carrying out your instructions. We will incur no liability to you if we delay, block or freeze any transaction or refuse to pay money if we reasonably believe that such transactions are in breach of the law.

13. Tax File Numbers & Non-resident withholding tax

Federal law treats interest earned on deposits as income and may be taxable, depending on your circumstances.

We will ask for your TFN when you open your first account with us. You do not have to disclose it or claim an exemption. If not disclosed or an exemption confirmed, we are required to deduct withholding tax at the highest marginal tax rate (plus the Medicare levy) from your interest payments.

For joint accounts, withholding tax will apply to all interest earned unless **each** account joint holder provides their TFN and/or exemptions.

For business use accounts, the Australian Business Number is required to avoid withholding tax.

If you are, or become, a non-resident for taxation purposes, we are required to deduct non-resident withholding tax from any interest payments made to you. If you notify us of a change of your residential or mailing address to an overseas address, we will assume that you are no longer resident for taxation purposes and will commence deducting withholding tax unless and until you advise us not to.

14. Opening a joint account

You may open an account jointly with another member.

You can nominate the account to be operated by "any to sign", "any two to sign" or "all to sign". If you do not make a nomination it will be operated with "any to sign".

A joint account holder may only make a withdrawal on the terms of the operating authority. If you tell us there is a dispute between joint account holders or any joint account holder requests us to change the operating authority so that all joint account holders must approve future withdrawals or a joint account holder requests us to suspend the account, we will comply with the request until we receive an updated operating authority or instructions to disperse the funds from both parties (these instructions can be provided by sending us a Secure Mail message via your Internet Banking or by contacting our Member Experience Centre).

An "any two to sign" or "all to sign" will restrict access to the joint account:

- by requiring written signatures; or
- through our Member Experience Centre by providing your access codes; and
- we will not allow transactions to be performed using a card, Phone Banking, Mobile Banking or Internet Banking (however, we may permit information only access to your account if this is required).

The important consequences of holding a joint account are:

- the credit balance of a joint account is held jointly by all account owners so that **each** account holder has the right to the entire balance, jointly with the other account holders.
- if a joint account holder dies, the surviving account holder is entitled to the credit balance (jointly if there is more than one survivor).
- the liability of account holder under an account held in joint names is joint and several. This means each and all account holders are liable for the whole of any debit balance on the account. We can sue all or any account holders for an amount owing on the account.
- Any joint account holder can authorise or manage Consumer Data Right data sharing arrangements.

For joint accounts, each account holder is entitled to receive a copy of any notice or other document issued. Where you do not wish to each receive separate copies of notices and other documents relating to your account, you may nominate one account holder to receive them on behalf of all account holders. If you make such a nomination and you are not the person nominated, you give up the right to be provided with information direct from us. However, any account holder can advise us at any time in writing to cancel the nomination and we will issue separate notices and other documents to all account holders from that date. To set up a nominated account holder please contact us.

15. Opening an account for a minor

Accounts for minors are opened in the minor's name provided the minor is a member. A parent, legal guardian or other adult acting on behalf of the minor may open a membership and accounts for the minor.

When you open a membership and account on behalf of a minor:

- you acknowledge that any credit balance held in the account is the property of the minor;

- you may operate the account as or appoint an authorised user in accordance with **clause 17**;
- the minor can access the account at the earlier of us receiving your written consent or once the minor is 18 years of age;
- you may authorise the minor to have access to the account at any time after the minor is 12 years of age and can register a consistent signature (in exceptional circumstances we may consider such a request for minors under the age of 12); and
- once the minor is 18 years of age, the minor will have automatic access to the account by presenting sufficient identification and registering a signature with us.

Operating restrictions apply to all accounts held under the minor's membership. For a list of operating restrictions applicable to minors please contact us by sending us a Secure Mail message via your Internet Banking or by contacting our Member Experience Centre. This means:

- When you authorise the minor to have access to the account, or when the minor claims access to an account at the age of 18, they can access and operate all accounts held under their membership. We will then remove your authority to operate any of the accounts under the minor's membership.
- If you are opening an account on behalf of a minor and do not wish the minor to gain automatic access to the account in accordance with this clause, you may consider opening an account in your own name and hold the funds on behalf of the minor. However, there may be tax implications for any credit interest earned on funds deposited to the account.
- Minors over the age of 12 may open and operate an account in their own name and without permission from a parent or legal guardian. If you had previously opened the membership/account on behalf of the minor, the minor will not be able to open a new account until you authorise the minor to have access to their membership. If this situation applies to you, please contact us to discuss the options available to you and the minor.

16. Opening an account for a trust

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 terms of the trust; and
- you agree to indemnify us against any claim made upon us in connection with the trust. However, you are not liable to indemnify us against any claim to the extent that it was caused by our mistake, fraud, negligence or wilful misconduct.

17. Authorised users

17.1 Account operating authority

You can appoint, remove or change the details, of an authorised user at any time by notifying us in writing.

For joint accounts, regardless of the joint account operating authority (refer to **clause 14**), all joint account holders must sign the request to appoint an authorised user. However, any account holder may request an authorised user to be removed.

17.2 Who can operate your account?

This table illustrates how your account will be operated when you appoint authorised users:

Type of account	Account operating authority	Who may operate the account?
Joint account	Any to sign	Any account holder or authorised user.
Joint account	Any two to sign	Any two of the account holders and/or authorised users.
Joint account	All to sign	All account holders and all authorised users.
Single account	Any two to sign	Account holder and any authorised user (if more than one authorised user is appointed). Example: Where you open an account on behalf of a minor over the age of 12 and authorise the minor to have restricted access to the account with an adult.
Single account	All to sign	Account holder and all authorised users.

18. Switching accounts

We can help you switch your accounts from another financial institution to us by contacting them to obtain the previous 13-month list of your direct debits (e.g. gym memberships or regular utility payments) and direct credits (e.g. your salary). This will not include any 'Pay Anyone' payments, BPAY payments or recurring payments where you have supplied your Visa card number. If you need further information, please contact us.

You agree that an authorised user can operate your account and conduct any transactions on it that you could do yourself and we can act on their instructions, for example:

- obtaining balance details;
- making withdrawals;
- authorising auto transfers and direct debits; and
- using electronic and other means of access to your account.

An authorised user cannot apply for a loan or increase the credit limit of a loan, change the type of access method issued to you, nominate additional authorised users, open accounts or close accounts.

You are responsible for:

- ensuring that the authorised user receives and reads a copy of these terms and conditions;
- the transactions of the authorised user on your account;
- ensuring the conduct of the authorised user complies with these terms and conditions; and
- the authorised user's registration for and use of any access method and access service.

17.3 Validity and expiry of the third-party signatory authorisation

If you cancel an authorised user's authority, you are responsible for all transactions conducted by the authorised user prior to cancellation and you must arrange return of any cards and access methods provided to them. We are not liable for any loss or damage caused by any delay in processing a cancellation of the authority, except to the extent that the loss or damage was caused by our mistake, fraud, negligence or wilful misconduct

We are not liable for any loss or damage caused to you by authorised users except where it arises from fraudulent conduct by our agents or employees, or if we are liable under a law or the ePayments Code.

Part 3
How to operate your account & access services

19. Table of accounts and access services

This table (see over page) provides a summary of key features and access services that may be permitted on deposit accounts subject to the account operating authority and these terms and conditions.

Refer to the ***Deposit Accounts Fees and Charges*** and ***Deposit Accounts Interest Rates*** brochures for full details of applicable fees and interest rates.

Account type	Access Account	55+ Account	Educator+ Account	Home Loan Offset Account	Association Account	Netsave Account	Bonus Savings Account	Children's Savings Account	Term Deposit	Home Equity & Line of Credit	Land Agents' Trust Account
Eligibility	All members	Members aged 55+	Education community	Eligible home loans	Not for profit organisations	All members	All members	Members <18 years of age	All members	No longer available	
Minimum opening deposit	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	$1,000	Nil	Nil
Minimum ongoing balance	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	$1,000	Nil	Nil
Minimum withdrawal amount	Nil	Nil	Nil	Nil	Nil	Nil	Nil	Nil	$1,000	Nil	Nil
Deposit term	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Varies[1]	N/A	N/A
Funds available at call	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Card access	Visa or rediCARD	Visa or rediCARD	Visa card	Visa or rediCARD	Deposit only	Deposit only	Deposit only	Visa or rediCARD[2]	✗	Visa or rediCARD	✗
Optional overdraft	✓	✓	✗[3]	✓	✗	✗	✗	✗	✗	✗	✗
Monthly access fee	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Transaction/ withdrawal fees	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Interest calculated on daily closing balance	No interest	Using stepped balances	✓	Offset against linked loan	✓	✓	✓	✓	✓	No interest on credit balances	No interest
Interest paid	N/A	Monthly	Monthly	N/A	Monthly	Monthly	Monthly	Monthly	Varies[1]	N/A	N/A
Statement frequency	Six monthly	Six monthly	Six monthly	Six monthly	Monthly	Six monthly	Six monthly	Six monthly	Six monthly	Monthly	Monthly
ATM withdrawals and transfers	✓	✓	✓	✓	✗	✗	✗	✓[2]	✗	✓	✗
Automated transfers (periodical payments)	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
Bank@Post withdrawals and deposits	✓	✓	✓	✓	Deposit only	Deposit only	Deposit only	✓[2]	✗	✓	✗
BPAY payments	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
Branch withdrawals, transfers and deposits	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Direct credits	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Direct debits	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗
EFTPOS purchases and cash out	✓	✓	✓	✓	✗	✗	✗	✓[2]	✗	✓	✗
Internet, Mobile and Phone Banking transfers	✓	✓	✓	✓	✓	✓	✓	✓	View only	✓	✓
Member Contact Centre transfers	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
NPP Payments	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Round Up Origin Account	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Round Up Destination Account	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Visa debit purchases online, using payWave and EFTPOS	✓	✓	✓	✓	✗	✗	✗	✓[2]	✗	✓	✗

[1] Refer to clauses 22.3 and 29 for full details.

[2] Full card access is permitted where the child is authorised to operate the account independently. Deposit-only card access may be permitted where the account is operated on behalf of the child. From 16 October 2023, rediCARDs will not be available to new members. Visa cards with operating restrictions for the use of the card will be issued as a default card for minors. Please see Clause 15 for further information about how age restrictions for minors in the Visa card operate.

[3] Not available to new accounts.

20. Making cash and cheque deposits to your account

Cash deposits can be made over the counter at a branch or Bank@Post. We or Bank@Post may impose limits on the amount and/or the denomination (coins) of cash deposits. Please contact us or your nearest Australia Post outlet for details of any limits that apply.

Cheque deposits can be made at Bank@Post. Please contact your nearest Australia Post outlet for details of any limits that apply.

We use your account number only when processing deposits. We do not check the account name received with the deposit instruction.

Members can deposit foreign currency cheques with Credit Union SA if they held a membership prior to 1 December 2022. Any new members after this point will not be able to access this service.

Cheques deposited via Bank@Post may take up to 10 business days to clear and overseas cheques will take considerably longer. Until cleared, the available balance will not include the amount of the cheque and you will not be able to withdraw the proceeds of that cheque.

All cheques become stale if they are presented for payment more than 15 months after the date on the cheque. Stale cheques will not be honoured for payment.

Cheques can normally only be paid into an account in the name of the payee. If you wish to deposit a cheque to your account and you are not the payee, ownership of the cheque must be transferred to you by having the payee transfer ownership and sign the reverse of the cheque. Even if you do this, cheques may be refused if there are any doubts that you are the rightful owner.

Cheques may be dishonoured or payments refused for the following reasons:

- insufficient clear funds in the payer's account;
- the cheque has not been signed;
- the cheque is stale (more than 15 months old);
- the cheque has a future date on it;
- the cheque has been altered in a material way and the alteration has not been signed;
- the cheque has been stopped by the drawer;
- the payer's bank has been notified that the payer is unable to manage its own affairs, is bankrupt or has died.

21. Making additional deposits to term deposits

You cannot make additional deposits to a term deposit before the term matures. You can deposit additional funds at maturity and prior to reinvestment of your term deposit.

22. Making withdrawals from your account

Unless stated otherwise in these terms and conditions, you can withdraw money from your account provided you have sufficient clear funds available in the following manner:

- cash at a branch or Bank@Post;
- electronic payment to a third-party supplier by direct debit;
- NPP Payments;
- by transferring funds to an account held with us by auto transfer or through Internet Banking, Mobile Banking, Phone Banking, our Member Experience Centre or a branch;
- by transferring funds to an account held with another financial institution by auto transfer or through Internet Banking, Mobile Banking, our Member Experience Centre or a branch;
- electronic payments to a third party using BPAY payments through Internet Banking, Mobile Banking or Phone Banking;
- electronic payments to a third party using Osko Payments through Internet Banking or Mobile Banking;
- if you have a card, by withdrawing cash or transferring funds to another linked account with us at ATMs and purchasing goods and/or withdrawing cash at EFTPOS terminals (if permitted by the operator of the terminal);
- if you have a Visa card, by purchasing goods using payWave at EFTPOS terminals (if you have a compatible digital wallet), purchasing goods online using your card or a digital wallet; or
- in any other manner we permit (if we do so, we can set further terms and conditions for those withdrawals).

We require proof of your identity (or any authorised user) before processing withdrawals made in person.

22.1 When making withdrawals with your card

You can authorise card transactions in the following manner:

- by using your Visa card alone or together with your PIN and either in physical form or via a digital wallet along with any electronic equipment including a contactless EFTPOS terminal;
- by presenting your rediCard or Visa card to a merchant and signing a voucher or other documentation authorising the transaction;
- by giving your Visa card details to a merchant or to any other party to whom payment is to be made either directly or through a third party (for example, purchasing goods over the phone or online); or
- by arranging an electronic debit on your Visa card by giving a standing authority to have payments made directly from your linked account.

When using a card to make withdrawals at:

- ATMs and EFTPOS terminals, you may only access your first nominated savings account;
- rediATMs, you may also access your second nominated savings account; and
- Bank@Post terminals, you may access your first nominated savings account by pressing 'savings', your second nominated account by pressing 'cheque' or your nominated loan account by pressing 'credit'. You need to notify us if you wish to access a second savings account and/or loan account.

22.2 Withdrawal limits

Withdrawal transactions are subject to the following daily and/or each transaction limits.

Access method or service	Transaction Type	Transaction limits
Over the counter at a branch	Cash withdrawal	Up to $3,000 per day. Note: You must give us at least one business day advance notice if you wish to withdraw cash in excess of this limit).
rediCARD	ATM withdrawals or transfers EFTPOS purchases (including cash out) where you select 'savings' or 'cheque' account. Bank@Post withdrawals.	Combined maximum of $2,000 per day for all the transaction types.
Visa card (cashless)	Where you select 'credit' account or make purchases for goods or services online. EFTPOS purchases (not including cash out) where you select 'savings' or 'cheque' account.	Up to your available balance.
Visa card (cash withdrawal)	ATM withdrawals or transfers EFTPOS purchases (including cash out) where you select 'savings' or 'cheque' account. Bank@Post withdrawals.	Combined maximum of $2,000 per day for all the transaction types.
Visa card, device with a digital wallet	payWave	$200 per transaction and a maximum of $1,000 per day (subject to a maximum of 20 transactions per day). Note: If you exceed the maximum number or value of payWave transactions, you can still perform transactions using payWave by entering your PIN.
Internet Banking and Mobile Banking	BPAY payments Transfer funds to another account held with us Transfer funds to an account with another ADI Transfer funds to an account with an overseas financial institution	Up to $10,000 per day Up to $25,000 per day Up to $5,000 per day Up to $5,000 per day
Phone Banking	BPAY payments Transfer funds to another account held with us	Up to $5,000 per day Up to $10,000 per day
Osko Payment or NPP Payment	Transfer funds to another account held with us Transfer funds to an account with another ADI	Up to $25,000 per day Up to $5,000 per day
Internet Banking	Business Banking batch transactions	Up to $25,000 per day

We may allow you to increase the transaction limits on a temporary or permanent basis.
If we do so, you will need to comply with any additional security requirements we may impose before we will increase your limit.

22.3 Withdrawals from term deposits

If you wish to redeem your deposit before the expiration of the agreed term, you must give us one business day advance notice and a minimum of $1,000 must be withdrawn. Refer to the ***Deposit Accounts Fees and Charges*** for the fees and charges and reduction in interest that may apply for early withdrawal of a term deposit.

If your deposit falls below the minimum ongoing balance requirement, the deposit will be redeemed in full, together with any accumulated interest, and transferred to an account in your name. If you do not hold an account with us, we will transfer the funds to another institution via EFT.

23. Overdrawing your account

You must not make a withdrawal transaction of any type that would exceed your available balance. If you schedule or attempt to make a withdrawal of any type that would cause you to exceed your available balance, we may do any of the following:

- dishonour the payment;
- honour the payment and allow you to exceed your available balance; or
- if you have sufficient funds available in another account, transfer funds between your accounts to enable the payment to be made without overdrawing your account or exceeding your credit limit.

If you have scheduled or attempt to make more than one withdrawal that would cause you to exceed your available balance, we may determine the order in which payments will be made and treat each payment differently (for example, we may honour one payment and dishonour another).

We have no legal obligation to notify you if we dishonour a payment due to insufficient funds. We are not liable for any loss suffered by you or another as a result of a payment instruction being dishonoured (including where we do not notify you that payment has been dishonoured due to insufficient funds).

If we honour a payment and allow you to overdraw your account, you will incur a debt to us of the amount by which the payment exceeds your available balance. You must repay that debt immediately.

If your account is overdrawn, interest is calculated daily by applying the daily percentage rate to the unpaid daily balance of the account and is debited to the account on the last day of the statement period.

The daily percentage rate is determined by the variable Overdraft interest rate, as per the ***Personal Loan and Visa Credit Card Interest Rates and Fees and Charges*** brochure.

24. Processing transactions

We debit the value of all withdrawal transactions from your account and credit the value of all deposit transactions to your account, in accordance with your instructions and with these terms and conditions. Transactions will not necessarily be processed to or from your account on the same day. We will process transactions on any one day in any order we determine.

When you or an authorised user makes an EFT transaction, it is your responsibility to tell us the correct amount you wish to pay or transfer, and the correct account you wish to have the payment or transfer credited to. The 'account name' will not be used to verify if the account details are correct.

We may be prohibited from effecting your instructions in relation to any transactions for any reasons including where you have insufficient available balance, or the transaction poses a security or credit risk to us or if we reasonably believe the transaction may be in breach of the law. We will not be liable to you or any other person for any loss or damage suffered as a result of delaying, blocking, freezing or refusing to give effect to your instructions, except to the extent that we acted unreasonably in doing so.

25. Account information

You can obtain information on your account by contacting our Member Experience Centre, visiting a branch or, where permitted for the type of account, using Internet Banking, Mobile Banking, Phone Banking or through your digital wallet.

25.1 Account statements

We will send you account statements at least once every six months or as otherwise set out in the **Table** in **clause 19**.

The statement will set out the details of the transactions on your account for that period. Unless you have registered for eStatements, you will receive your account statement by post at your nominated postal address we have on record.

We will send you a combined account statement if you have multiple accounts.

You can request for us to send you account statement(s) each quarter or month or reissue a previously issued statement.

You should carefully check your account statements. We will provide you with a receipt or receipt number for each transaction effected using a device. We recommend that you keep or note these to check the transaction against your account statement.

If you believe that there is an error (or mistake), unauthorised or disputed transaction, you should contact us immediately.

25.2 eStatements

We encourage you to view your account statements electronically through our eStatement service. You can register for eStatements through Internet Banking or via our Mobile Banking App, by contacting our Member Experience Centre or visiting a branch. When you register for eStatements, you will no longer receive your account statements by post. Your eStatements will be available via our Internet Banking and you will receive an email (at your nominated email address we have on record) that your account statement is available for viewing.

You can unsubscribe from receiving eStatements at any time.

25.3 SMS Alerts

SMS Alerts allow you to keep track of your account balances and transactions via your mobile phone. You can set alerts to report on specified events (or transactions), at regular intervals and/or to provide information on a one-off basis.

Event alerts will report via SMS to your mobile phone between 7am and 8pm daily. Any events that occur between 8pm and 7am will report after 7am.

You can register for the SMS Alerts service through Internet Banking or via our Mobile Banking App, by contacting our Member Experience Centre or visiting a branch. By registering for the SMS Alerts service, you authorise us to:

- send your account information to the mobile number you have nominated; and
- process your account information outside Australia using transmission equipment outside Australia that may store your information in the circumstances where you are overseas and you do not deregister from the SMS Alerts service.

We have no control over who can access your account information once we have sent the SMS alert. To protect information sent via SMS Alerts, you should:

- keep your mobile phone in a secure and safe place at all times;
- delete SMS alerts from your mobile phone once you have read them; and
- contact us immediately if your mobile phone is lost or stolen or if your mobile phone number has been disconnected, changed or suspended.

SMS alert history can be viewed in Internet Banking. You can deregister from the SMS Alerts service at any time.

We will try (without any legal obligation) to provide the SMS Alerts service. This service is available to you at the specified times, providing that the information about your account is accurate and current. Circumstances may not always make this possible.

We do not charge you a fee for the SMS Alerts service. Your telecommunications provider may charge you a fee for receiving the SMS alerts.

26. Fees and charges

Refer to the ***Deposit Accounts Fees and Charges*** brochure for full details of current fees and charges. We may vary our fees and charges in accordance with **clause 34**. We will debit your primary operating account for all applicable government taxes and charges and any fees.

27. How interest is calculated and paid on savings accounts

Refer to the ***Deposit Accounts Interest Rates*** brochure for full details of current interest rates.

For all interest-bearing savings accounts, we calculate the interest on the daily closing balance using the annual interest rate divided by 365 and pay interest on the last calendar day of each month.

For all interest-bearing accounts other than the 55+ Account, interest will be calculated for a particular day by applying a single annual interest rate regardless of the balance of your account. The interest rate used to calculate interest for a particular day may depend on the balance of your account (outlined in the ***Deposit Accounts Interest Rates*** brochure) and/or whether you meet the eligibility requirements for bonus interest outlined in this clause.

The 55+ Account has a tiered interest rate. A tiered interest rate means that the annual interest rate applicable to your 55+ Account for a particular day will vary depending on the balance of your account on that day. For your 55+ Account, interest is calculated using:

- a single interest rate, if the balance of your account is equal to or below the upper limit of the first interest rate tier; or
- different interest rates for the portion of your account balance in each interest rate tier, if the balance of your account exceeds the upper limit of the first interest rate tier.

Bonus interest will apply to eligible savings accounts if the following conditions are met:

- for the Bonus Savings Account, bonus interest applies for each month where you make a deposit of any amount and no withdrawals and;

- for the Children's Savings Account, bonus interest applies for each month where you make a deposit of any amount and no withdrawals. The portion of any balance above $50,000 will not receive bonus interest.

28. How interest is calculated on Home Loan Offset Accounts

You must link your Home Loan Offset Account or Offset Account to an eligible home loan. You may link more than one offset account to an eligible home loan subject to these terms and conditions.

We do not pay any interest on the Home Loan Offset Account or Offset Account. Rather, we calculate interest payable on your linked loan on the daily balance of the loan as reduced by the daily balance of your Home Loan Offset Account or Offset Account. This reduces the amount of interest payable on the linked loan while you hold credit funds in your Home Loan Offset Account or Offset Account.

If the balance of your Home Loan Offset Account or Offset Account exceeds the balance of the linked loan, we will not pay credit interest on the portion of the balance exceeding the balance of the loan.

Where the linked loan is held in joint names, the Home Loan Offset Account or Offset Account may be held by any of the borrowers individually or any or all of the borrowers jointly. Home Loan Offset Accounts and Offset Accounts cannot be held by, or jointly held with, a person who is not a party to the linked loan.

If your Home Loan Offset Account or Offset Account is not linked to an eligible loan, including when your linked loan is repaid in full or becomes ineligible (for example, if you switch your loan to a fixed interest rate), we will not automatically close or transfer your account. We may choose to transfer your account to an Access Account and do not need to give you advance notice of our intention to do so (but we will notify you as soon as practicable thereafter), however we are not obliged to do so.

29. How interest is paid on term deposit accounts

The interest rate is fixed for the term of the deposit.

Interest is calculated on the daily closing balance and payable:

- at maturity, for terms of less than 12 months; and
- fortnightly, monthly, quarterly or annually for terms of 12 months or more.

30. Maturity of term deposits

You will receive a reinvestment notice from us before the maturity date of the deposit which sets out the details of the deposit and our rates applicable at the date of the notice. You should keep reinvestment notices upon renewal along with the original certificate of deposit.

Unless you have directed us otherwise your deposit will be automatically reinvested for the available term most closely matching your current term upon maturity.

Regardless of the rate quoted on the reinvestment notice mentioned in the first paragraph of this clause, you will receive the rate applicable at the time of your deposit maturity date (renewal date).

31. Our right to combine and set-off accounts

We may combine or set off the balances of two or more of your accounts or credit facilities to the extent required to pay any amount owing to us in respect of one of your accounts or credit facilities that has not been paid when it has become due and payable. We will have regard to any circumstances of financial hardship, of which we are aware, when considering whether to combine or set off balances. If we exercise our rights under this clause, we do not need to give you advance notice but we will notify you as soon as practicable afterwards.

32. Dormant accounts

A deposit account becomes dormant if it is not operated for 24 months or more consecutively. If all accounts within your membership become dormant, we will write to you asking if you want to keep your membership. If you do not respond within one month, we will treat your membership as being dormant. We will stop paying you interest, cancel any or all of your access methods and/or close your accounts and membership without notice to you.

If you have not made any transactions to your account (other than for accounts held in the name of a minor) for a period of seven years and the combined balance of your accounts exceeds $500, we may be required by law to send your money to the ASIC as unclaimed money. While you can reclaim your money at any time, we recommend that you operate your accounts regularly to avoid this inconvenience.

33. Resigning from your membership, closing your accounts or cancelling an access service

You may resign your membership, close your account or cancel any access services on request at any time by contacting our Member Experience Centre, by visiting a branch and, where permitted by the type of account or access method, using Internet Banking or Mobile Banking.

When you resign from your membership, you must close your account(s) with us and cancel the access service linked to your account. You must:

- securely destroy all cards used to access your accounts;
- cancel any direct debit authorities; and
- cancel any regular payment arrangement under your Visa card.

We may defer closure and withhold sufficient funds to cover payment of outstanding debits on your account. Where a Visa card is linked to one of your accounts, we will not end/close your membership and accounts for 31 days after your request has been received. We will then send you the balance of your accounts via EFT plus any amount you paid for your membership share (if any) and any accrued interest less any accrued fees and overdraft interest applicable up to the date of closure.

34. Changes to these terms and conditions

We may change fees, charges, interest rates and other terms at any time (provided that we may not make any changes to the terms applying to a term deposit account which will take effect prior to the end of its current term). Where we do so, we will give you notice that complies with the minimum requirements specified by law and any code of practice to which we subscribe. Where we notify you of changes to these terms and conditions, your use of the account or an access service after the notice period is deemed acceptance of the changes contained in that notice.

If you believe you will be adversely affected by the changes we intend to make, you may resign your membership, close your account or end your use of an access service by contacting our Member Experience Centre, by visiting a branch or, where permitted by the type of account or access method, using Internet Banking or Mobile Banking.

If we notify you our intention to increase a transaction limit and you do not wish your limit to increase, you should contact us and we will not apply the increase to you.

The following table sets out how we will give you advance notice of the change:

Type of change	Notice period
Increasing a fee or charge	20 days
Introducing a new fee or charge	20 days
Changing the method by which interest is calculated	20 days
Increasing your liability for EFT transactions	20 days
Imposing, removing or changing any periodic transaction limit	20 days
Changing any other term or condition regulated by the ePayments Code	20 days
Changing interest rates	On or after the day of the change, including when we next communicate with you
Changing any other term or condition	On or after the day of the change, including when we next communicate with you
Changes to Osko Payments unless the changes are: • required by law; or • to accommodate changes in the operations of the Osko Scheme operation or our operations and systems; or • to comply with our or BPAY's security policies and procedures.	30 days

We may not be able to give you advance notice in certain circumstances such as:

- where an immediate change is necessary to restore or maintain the security of our systems, access services or account, the prevention of systemic or individual criminal activity, including fraud; or
- to enable us to comply with the changes in the rules and regulations of access services which are owned and operated by third parties.

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

- notification by letter;
- notification on or with the next newsletter;
- media advertisements;
- notifications through Internet Banking or Mobile Banking App;
- notifications via email; or
- notification on our website.

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.

35. How we give you notices

We may give you any notice, statement or other document (including a notice of a change to these terms and conditions) in connection with your account or access service to you personally or, where permitted by law, by electronic means. Each of these methods of delivery constitutes written notice.

Electronic means may include:

- sending the document to your email address; or
- making the document available on our website, in our Internet Banking or our Mobile Banking app and sending you an email when the document is available to be retrieved.

We will use your contact information on our records. You must notify us whenever you change your contact details.

If we receive returned mail because you have not notified us of a change of contact details, we may place a stop on your account which restricts or limits your ability to transact on your account.

36. What happens if you change your personal details?

You must notify us if you change your name, residential or postal address, email address or contact numbers so that we can continue to contact you about your account and access services linked to your account.

37. Law and jurisdiction

These terms and conditions are governed by the laws of the State of South Australia. In relation to any proceedings about or in connection with your account, we and you agree to submit to the non-exclusive jurisdiction of the courts that have jurisdiction under that law.

Part 4
Specific conditions applying to access services

38. Access code

You can use an access code to make enquiries about your accounts, make changes to your accounts, update your personal and contact details, complete BPAY payments , external transfers and to transfer funds between your accounts through our Member Experience Centre.

You must nominate your access code when you apply for our access code service. By nominating an access code, you authorise us to act upon the request or direction of anyone who telephones us (and claims to be you) and quotes your access code.

You can cancel your access code at any time by contacting us.

39. Bank@Post

You can use Bank@Post to make deposits and cash withdrawals by using your card and PIN. You will not be able to make enquiries about your available balance, transfer funds between your accounts or make cheque withdrawals using Bank@Post.

You may access up to three accounts using Bank@Post. You will need to notify us of the accounts you wish to have access to using Bank@Post.

40. Business Banking

Business Banking is only available to business purpose accounts.

You can use Business Banking to group EFT transactions via the internet together into one batch for processing. You can also use Business Banking to allow funds transfers and withdrawals through Internet Banking for accounts with "two to sign" or "all to sign" authorities.

The two types of access available for a Business Banking facility are:

Types of access	Functionality
Full access	Create a batch Update any transaction within the batch Approve and process batch on "any to sign". Note: For "any to sign" or "all to sign", one or all other authorised users must authorise and process the batch.
Create & update only	Create a batch. Update any transaction within the batch.

You must be registered for Internet Banking before you can register for Business Banking.

Where batches are to be loaded against accounts that require multiple account holders to operate, each authorised user who is responsible for creating and/or approving batches must have the Business Banking service registered on their personal membership with us.

41. Cheques

41.1 Foreign Cheques

Members can deposit foreign currency cheques with Credit Union SA if they held a membership prior to 1 December 2022. Any new members after this point will not be able to access this service.

42. Direct credits and arranging for your income to go into your account

You can arrange for a third party (such as your employer) to direct credit funds to your account by providing them with our BSB number (805-007) and your account number. It is important that the account information you provide to the third party is accurate. If the account information you provide is incorrect, then the payment may be rejected or credited to another account. We are not liable for any loss you incur as a result of delays in the funds reaching your account or funds credited in error to another account due to incorrect account information.

If you want to change or cancel a direct credit, you must contact the organisation responsible for depositing funds to your account.

If you believe that your account has been credited for the wrong amount, you must contact the organisation responsible for depositing funds to your account to resolve the matter.

43. Direct debits

You can authorise a supplier to automatically debit funds from your account. The supplier will provide you with a DDR for you to complete and sign to provide them with this authority. You will need to provide the supplier with our BSB number (805-007) and your account number. The account information you provide to the supplier must be accurate. If it is incorrect then the direct debit may be rejected. We are not liable for any loss you incur as a result of your direct debit being rejected due to incorrect account information.

Once a DDR is established, we will continue making payments to the supplier for whatever amount is requested by the supplier provided you have sufficient available balance, unless you or we cancel the payment in accordance with this clause.

If you want to stop a direct debit, you must contact us at least five business days before the next payment is due. We recommend you also contact the supplier to avoid any fees for the dishonour of their direct debit.

If you want to cancel the DDR, you can either contact us or the supplier. If you contact us, we will cancel the DDR promptly. We can also cancel or suspend your direct debit facility for the reasons set out in **clause 56**. If we do so, the supplier may charge you a fee for each dishonour of their direct debit. We will not charge you a fee for cancelling the DDR.

We cannot reverse a payment once it has been made. If you believe your account has been debited for the wrong amount but there is a valid DDR in place, you must contact the supplier to resolve the matter.

If the supplier debited your account without a valid DDR or you have cancelled a prior DDR, you should contact the supplier to obtain a refund of the payment or to provide evidence of their continuing authorisation to debit your account. The process of resolving this disputed transaction is as follows:

- If the supplier can provide a valid DDR and you are unable to provide evidence that you had cancelled the DDR, you cannot lodge a claim with us.
- If the supplier attempts to debit your account as per your DDR and there is insufficient funds, you may incur a fee. (Refer to the Deposit Accounts Fees and Charges Brochure).
- If the supplier is unable to provide a valid DDR or does not respond to your request, you can lodge a claim for an unauthorised direct debit with us. If we believe that you have valid grounds to do so, we will lodge a claim with the supplier's ADI and the supplier's ADI must respond within seven days of receipt of your request and either:
  - the supplier responds by providing evidence of a valid DDR to their ADI within seven days, in which case your claim will be refused and we cannot pursue the matter any further on your behalf; or
  - the supplier is not able to provide evidence or does not respond to the providers request of a valid DDR to their ADI within seven days, in which case your claim will be paid.

44. Auto transfers (periodical payments)

You can arrange for a payment to be paid on a regular periodic basis to a third party by reference to their BSB and account number. You can set up an auto transfer facility through Internet Banking, by contacting our Member Experience Centre and quoting your access code or by visiting a branch.

You must give us clear and concise payment instructions to enable the auto transfer authority to be processed. We will forward

payments in accordance with your instructions and will continue making payments to the third party provided you have sufficient funds in your account, unless you or we have cancelled the payment in accordance with this clause.

If you want to stop an auto transfer or future-dated payment, you must cancel the payment before the next payment is due through Internet Banking, by contacting our Member Contract Centre and quoting your access code or by visiting a branch.

We may cancel or suspend an auto transfer authority for the reasons set out in set out in **clause 56** and where your payment has been rejected five times because of insufficient available balance. We recommend you contact the third party to avoid any fees that may apply if your payment is dishonoured.

45. Visa card and rediCARD

A Visa card or rediCARD may only be used to perform transactions on a linked account. We will debit your linked account with the value of all EFT transactions performed using your card. We will advise you from time to time what type of EFT transactions may be performed using a card and the type of electronic equipment and terminals that may be used.

From 16 October 2023, rediCARDs will not be available to new members.

45.1 Using Visa card with payWave

If you have a Visa card with the payWave indicator displayed on the front of your card, that means that your card is enabled to make contactless transactions and you do not need to swipe your card or enter your PIN to perform transactions. You can still enter your PIN at EFT terminals or provide your signature even if your card can make contactless transactions.

To make a purchase of $200 or less using payWave, you will need to place your card on or near the merchant's contactless terminal. You will not receive a receipt for the payWave transaction from the merchant unless you ask for it. Before you place your card, you should check that the transaction details are correct on the merchant's terminal and never hand over your card to the merchant.

If you have exceeded the number or amount of payWave transactions permitted per day, you can still perform payWave transactions, but you will need to enter your PIN to complete the transaction.

45.2 Using Visa card with digital wallet

Your Visa card may be used with a digital wallet that we approve for use to make contactless payment to merchants and payments within digital wallet applications. We will need to identify and verify your identity before you register your Visa card into a digital wallet.

By registering for a digital wallet, you agree that we may exchange information about you with the digital wallet provider and Visa to enable the use or the improvement of the digital wallet and provide you with information about your digital wallet transactions.

There may be additional terms and conditions issued by the digital wallet provider and your telecommunications provider, and you are required to comply with them. We are not the digital wallet provider. We are not responsible for the use or function of the digital wallet (including any disruption, failure, malfunction or unavailability or security breach affecting information stored or sent from the digital wallet). You must direct questions about the use or functionality of the digital wallet to the digital wallet provider.

If you access your mobile device with a biometric identifier, you will not be required to provide your device's passcode to make payment through the digital wallet on your mobile device.

If you want to remove your Visa card from the digital wallet at any time, you must follow the procedures set by the digital wallet provider for removing cards.

We may prevent you from adding your Visa card to a digital wallet, suspend your ability to use your Visa card to make purchases using a digital wallet, or cancel your ability to use your Visa card in a digital wallet:

- for the reasons set out in **clause 56.2**;
- where you ask us to suspend or cancel your card; and/or
- we are directed to do so by the digital wallet provider or Visa.

We do not warrant that merchants will accept payments by digital wallet. We are not liable to you for any loss you suffer if a merchant refuses to accept a digital wallet. We can cease to support digital wallets at any time.

If we do, we will give you whatever notice, if any, is reasonable taking into account the reasons why we are ceasing to support digital wallets.

WARNING: Your mobile device may be linked to other devices by a common account.

If so, when you add your Visa card to a digital wallet using the mobile device, your card may also be accessible through a digital wallet on a linked device and may permit users of those devices to see your card information and make payments with your card.

Please contact your digital wallet provider for more information.

45.3 Using your card overseas

You can use your Visa card or rediCARD to purchase goods and withdraw funds from electronic equipment overseas. You can also purchase goods online from an overseas merchant using a Visa card (but not a rediCARD). All transactions made in a foreign currency will be converted into Australian currency by Visa 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 date on which Visa processes the transaction.

A currency conversion fee applies to all transactions made in a foreign currency. Please refer to Deposit Account Fees and Charges Brochure for futher details.

Overseas merchants and electronic terminals may charge a surcharge for making EFT transactions. Once you have confirmed the transaction, you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.

You will be charged a 3% currency conversion fee on the following types of transactions:

- A multi-currency transaction - where you make a purchase in a currency other than AUD (either over the phone, in person, or online).
- Single Currency - for online purchases where the merchant or their acquirer is located overseas but they accept payments in Australian Dollars.
- Dynamic Currency Conversion - where you make payment (in person), and the merchant converts the amount to Australian Dollars (AUD).

NOTE: It is not always possible to ascertain whether it is the merchant or the processing entity that is located overseas. Shopping websites with a domain name that ends in '.com.au' may appear to be an Australian business, but they or their bank may be located overseas and you may be charged a currency conversion fee.

Before travelling overseas, you should tell us the destinations that you intend to use your card. Otherwise, we may refuse to accept payment instructions as part of our security transaction monitoring procedure where we identify those instructions as being inconsistent with your usual transaction behaviour. You must comply with all applicable exchange control and tax laws governing the use of the card and you indemnify us against liability, loss, fees, charges or costs arising as a consequence of a failure to comply with them.

45.4 Using your card to make regular payment arrangements

You can authorise your card to be used for regular payment arrangements to merchants. You should keep a record of any regular payment arrangement that you have entered into with a merchant. You can ask us for a list of any regular payment arrangement for up to the previous 13 months.

We will continue making payments to the merchant for whatever amount is requested provided you have sufficient available balance and unless you or we cancel the payment in accordance with this clause.

If you want to change or cancel a regular payment arrangement, you must contact us or the merchant at least 15 days before the next scheduled payment. You should keep a copy of the change or cancellation request.

If your card details have changed (for example, your card was lost, stolen, or expired and has been replaced), you must ask the merchant to change the details of your existing regular payment arrangement to ensure that they continue. If you don't, your regular payment arrangement may be dishonoured and/or the merchant may stop providing you with the goods and services.

If your card or linked account is closed or suspended for any reason, you must notify the merchant immediately to change or cancel your existing regular payment arrangement or the merchant may stop providing you with the goods and services.

45.5 Round Up on your card transactions

The Round Up feature allows you to round up the amount of eligible Round Up transactions (defined below) to an agreed amount. The amount by which the transaction is rounded up will be automatically transferred from the origin account to the destination account as a separate transaction.

For example, assume the Round Up amount is $1. You purchase coffee using payWave for $3.50 from your origin account. We will then debit $3.50 and $0.50 from your origin account, paying the merchant $3.50 and transferring $0.50 to your destination account.

Eligible origin accounts are our Access Account, 55+ Account, Home Loan Offset Account and Educator+ Account

Eligible destination accounts are defined in the **Table** included in **clause 19** of these terms and conditions). The destination account must be in the same name as the origin account that has been registered for Round Up. For joint accounts, the destination account can be in either or both names of the account holders if the account is "any to sign". Round Up is not available on joint accounts with "any two to sign" or "all to sign".

Eligible Round Up transactions are:

Visa card transaction	Eligible Round Up transaction	Important things for you to know
In-store purchases made with your Visa card including cash outs	✓	Round Up amount is calculated on the Australian dollar value of the transaction. Round Up amount will not be debited if it causes the available balance on your linked account below $0.
payWave	✓	
Digital wallet	✓	
Online, telephone or mail order purchases using your card number	✓	
Regular payment arrangements using your card number	✓	
Bank@Post withdrawals	✓	
Chargebacks (where the merchant reverses an eligible Round Up transaction)	✗	Transfer of the Round Up amount **will not** be reversed
Reversals (where we reverse an eligible Round Up transaction)	✗	Transfer of the Round Up amount **will** be reversed

Transactions not made using your Visa card, including BPAY Payments, electronic transfers of any type, direct debits and staff -assisted transactions, are **not** eligible Round Up transactions.

If you have sufficient available balance in your origin account to perform the requested transaction but the Round Up amount would cause your account to become overdrawn, the transaction will still be processed and the Round Up amount for that transaction will be $0.

You must register for Round Up through the Mobile Banking App. To register for Round Up you must nominate an origin account and
a destination account. By registering for Round Up, you authorise us to debit the rounded-up amount from your origin account as a separate transaction.

You can also deregister for Round Up through the Mobile Banking App or by contacting our Member Experience Centre.

We may suspend or cancel Round Up if your origin or destination account is closed or for the reasons set out in **clause 56.2**.

45.6 Withdrawal and transaction limits

In addition to the daily transaction limits that apply in **clause 22.2**, we may at any time limit the amount of an EFT transaction if this is required for security or credit risk purposes. You acknowledge that third party organisations including merchants may impose additional restrictions on the amount of funds that may be withdrawn, paid or transferred.

45.7 Card renewal

New cards are automatically reordered before the expiry date of your existing card unless:

- you are in breach of these terms and conditions;
- we determine, on reasonable grounds, that you should not be issued with a replacement card for the security of us or your account; or
- we are not satisfied, on reasonable grounds, with the conduct of your account.

If you do not wish to receive a replacement card, you should contact us before the current card expires.

45.8 Card cancellation

Any cards that we issue remain our property. You may cancel your card at any time by contacting us.

We may cancel a card and demand its destruction either immediately if we deem it necessary for security reasons, on reasonable grounds, or by giving you 30 days advance notice for any other reason (which we are not required to specify).

You are liable for any transactions you make using the card before it is cancelled but which are not posted to your linked account until after cancellation of the card.

You must destroy your card when:

- we notify you that we have cancelled the card;
- you close your linked account(s);
- you resign your membership;
- you cancel your card; or
- you change the operating authorities of your linked account(s) (for example, you change your account to "all to sign") unless we agree otherwise.

45.9 Lost card

Where you lose or misplace your card, and you request for a new card to be issued, a fee will apply. Refer to the Deposit Accounts Fees and Charges brochure.

45.10 Using your card after cancellation or expiry

You must not use the card either before the valid date or after the expiration date shown on the face of the card or after the card has been cancelled. You are liable to reimburse us for any indebtedness incurred through such use whether or not you have closed your linked account(s) with us.

45.11 Exclusions of warranties and representations

We do not warrant that merchants or ATM terminals displaying card signs or promotional material will accept your card. We are not responsible if a merchant, bank or other institution displaying card signs or promotional material refuses to accept or honour your card.

We are not responsible for any defects in the goods and services acquired by you through the use of the 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. Where you have authorised a merchant to transact on the account by providing your card number or used your card to make a purchase, you may be entitled to reverse (chargeback) the transaction where you have a dispute with the merchant. For example, you may be entitled to reverse a transaction where the merchant has not provided you with the goods or services you paid for and you have tried to get a refund from the merchant and were unsuccessful.

To avoid losing any rights you may have for transactions other than unauthorised EFT transactions you should:

- tell us within 30 days after the date of the transaction; and
- provide us with any information we ask for to support your request.

Please contact us for more information about your chargeback rights.

46. Phone Banking

Phone Banking is our automated service enabling you to obtain information and perform selected transactions on your accounts using a telephone and password.

You can access Phone Banking by calling **1300 134 636.**

You must give us clear and concise instructions when using Phone Banking. We may vary the services we make available and/or which of your accounts may be accessed using Phone Banking, at any time and without prior notice to you.

47. Internet Banking

Internet Banking enables you to obtain information, change your personal and contact details, send secure communications, perform selected transactions on your accounts and perform a range of other services using a passcode on a computer or mobile device with access to the internet. We may vary the services we make available and/or which of your accounts may be accessed using Internet Banking, at any time and without prior notice to you.

For joint accounts that operate on an "any two to sign" or "all to sign", you will not be able to transfer funds or make payments in Internet Banking.

47.1 How to register for Internet Banking

You can register for Internet Banking using our online membership application form (as part of your application to become a member), by contacting our Member Experience Centre or by visiting a branch. We may introduce additional means to apply for Internet Banking from time to time.

If you register for Internet Banking through our online form, you will be responsible for nominating your initial password. If you register for Internet Banking through our Member Experience Centre or via a branch, we will supply you with a default password that must be changed the first time you log on to Internet Banking. We recommend that you choose a complex password comprising a combination of letters (both uppercase and lowercase), numbers, symbols and special characters.

Remember: to protect your account from unauthorised transactions occurring (where you may not be able to recover the funds) you must NOT use a password that resembles your birth date or part of your name.

47.2 Restricted transactions and functions

If you would like to add an extra layer of security to your account, you should register for Secure SMS (see **clause 49**) or VIP Security (see **clause 50**) to authorise restricted transactions (such as making payments to a new payee) and protected functions (such as updating your contact details) in Internet Banking.

Once you have registered for Secure SMS or VIP Security, we will send you a secure one-time code which must be entered prior to completing a restricted transaction or protected function in Internet Banking. Both Secure SMS and VIP Security are session based. This means that you are validated once you successfully enter a secure one-time code in an Internet Banking session.

If you exceed the allowable number of attempts to enter a secure one-time code when performing a restricted transaction or protected function, you will be locked out of either Secure SMS or VIP Security (depending on which layer of security you have selected) and will need to contact us to unlock Secure SMS or VIP Security.

You may make repeat transfers or payments to payees and billers that you have previously registered on Internet Banking without entering a secure one-time code, except where it is a transfer to an overseas financial institution where a code is required for each payment. However, if there is a change to the biller or payee details (other than the transaction amount), you will need to enter a secure one-time code.

We may add or remove restricted transactions or protected functions in Internet Banking at our discretion without giving you advance notice.

48. Processing Phone Banking and Internet Banking transfers and payments

When we make a payment on your behalf, we are not acting as your agent or as agent to the payee to whom the payment is directed. You should allow time for your requested payment to be received and processed by your requested payee.

Transactions (except BPAY and international transfers) which are made on a business day up to the cut off time should be processed that day. Transactions (except BPAY and international transfer) which you make on a non-business day or after the cut off time should be processed on the next business day.

You must provide us with clear and accurate instructions when using Phone Banking or Internet Banking. You will be responsible for any mistakes that are entered. Once a payment or transfer has been made, we are unable to reverse the transaction. However, we may be able to recover the payment if it is a mistaken internet payment (see **clause 62**).

We will try (without any legal obligation) to provide Phone Banking and Internet Banking 24 hours a day, 7 days a week, but circumstances may not always make this possible. If Phone Banking or Internet Banking cannot be accessed at any time, we will try to give you advance notice.

49. Secure SMS

Secure SMS sends a one-time passcode to your mobile phone that must be entered to complete a restricted transaction or protected function. The one-time passcode is active for five minutes after it has been sent. You can receive Secure SMS one-time passcode if you have a landline phone that can receive text to voice messages.

If you are overseas, you can still use Secure SMS to make transfers and payments if your mobile phone and SIM card allow global roaming and the country you are in operates via a compatible network to your SIM card provider. If this will not apply to you or you are unsure, you should apply for VIP Security before going overseas.

You can view the history of your Secure SMS via Internet Banking. You should review your Secure SMS history.

To register for Secure SMS, log in to Internet Banking, select 'Security' from the menu and then choose 'Secure SMS management'. You must ensure you have the correct phone number listed on your personal information recorded on Internet Banking before clicking 'Register'. If incorrect phone numbers or no phone numbers display for selection during the registration process, you will need to contact us to update your phone number.

If you deregister from Secure SMS, you will not be able to perform restricted transactions or protected functions in Internet Banking.

50. VIP (VeriSign Identity Protection) Security

VIP Security is the highest level of security we offer for Internet Banking transactions and payments. VIP Security is made up of the following two options:

- VIP Access for Mobile; and
- VIP Security Token.

These options are referred to as VIP Security credentials. Both credentials generate one-time passcodes that can be used to authorise restricted transactions and protected functions in Internet Banking.

VIP Access for Mobile is a free application that you can download from the App Store or Google Play on your mobile device. Once you've downloaded VIP Access for Mobile and completed the registration process, your mobile phone will be able to generate one-time passcodes.

VIP Security Tokens are devices that generate one-time passcodes. If you have an existing VIP Security Token issued by someone other than us (for example an online merchant or another financial institution), you may be able to register the token for use with us, providing it is a VIP Token.

You will need VIP Security if you wish to permanently increase the limits for your transfers to other financial institution and/or BPAY payments made though Internet Banking (including Mobile Banking).

In order to activate VIP Security, you must first register for Secure SMS. You must then register your VIP Security credential in Internet Banking. A VIP Security credential can be registered against more than one membership. If you have previously registered for Secure SMS, you should deregister from Secure SMS once you have registered for VIP Security. If you do not deregister from Secure SMS, you may be required to enter a VIP Security generated one-time passcode and a Secure SMS generated one-time passcode when performing a restricted transaction or protected function.

You can deregister your VIP Security credential (VIP Access for Mobile or Token) through Internet Banking. If you deregister from VIP Security, you will not be able to perform restricted transactions or protected functions until you register for Secure SMS. If you had increased your daily transaction limits for your transfers to other financial institutions and/or BPAY payments made through Internet Banking, then on deregistration from VIP Security, those limits will revert to the existing limits we permit.

51. BPAY

You can use BPAY through Phone Banking, Internet Banking and Mobile Banking.

51.1 Using BPAY

We are a member of BPAY. We will tell you if we are no longer a member of BPAY. BPAY can be used to pay bills bearing the BPAY logo. We will advise you if and when other transactions can be made using BPAY.

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 (e.g. your account number with the biller), the amount to be paid and the account from which the amount is to be paid. If the payment is a future-dated payment, you must also tell us the date(s) on which you request us to make the payment.

If you instruct us to make any BPAY payment but close the account to be debited before the BPAY payment is processed, you remain liable for any dishonour fees incurred in respect of that BPAY payment.

You acknowledge that:

- third party organisations (such as billers or other financial institutions) may impose additional restrictions on your access to and use of BPAY.
- 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.

51.2 Processing of BPAY payments

A BPAY payment instruction is irrevocable. Except for future-dated BPAY payments (see **clause 51.3**), you cannot stop a BPAY payment once you have instructed us to make it and we cannot reverse it.

We will treat your BPAY payment instruction as valid if, when you give it to us, you use the correct access method.

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; and
- otherwise, on the next business day after you direct us to make it.

The BPAY payment may take longer to be credited to a biller if you tell us to make it on a day other than a business day, or if another participant in BPAY does not process a BPAY payment as soon as they receive its details. Notwithstanding this, a delay may occur processing a BPAY payment if:

- there is a public 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 business day or after the cut off time on a business day; or
- a biller, or another financial institution participating in BPAY, does not comply with its BPAY obligations.

If we are advised that your payment cannot be processed by a biller, we will let you know and credit your account with the amount of the BPAY payment. We will take reasonable steps to assist you in making the BPAY payment as quickly as possible.

51.3 Future-dated BPAY payments

You may set a future payment date for a BPAY payment using:

- Phone Banking, up to 60 days after the date you are entering the transaction; or
- Internet Banking or Mobile Banking, at any date in the future.

If you use the future-dated BPAY payment you should be aware that:

- you are responsible for maintaining sufficient available balance 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; and
- 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).

We may limit the amount you may transact on any one day via BPAY on the other transactions, in addition to the limits outlined in **clause 22.2**. Individual billers can set transaction limits for payments and these can vary from time to time. These will override our daily limits if they are set lower than our limits.

51.4 Mistaken or unauthorised BPAY payment

You must nominate 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 paid and the amount you needed to pay.

You must notify 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.

If you believe a BPAY payment in your statement is wrong, or was not authorised by you, you must contact us immediately and provide any information that we reasonably require.

We will investigate your complaint in accordance with the timeframes set out in **Part 6** and subject to the provisions of **clause 63** concerning your liability for mistaken payments.

We will find that an error has been made if a BPAY payment is made to a person or for an amount which was not in accordance with your instructions to us or which we are satisfied that you did not authorise.

51.5 Your liability for BPAY payments

You are liable for all transactions carried out through BPAY by you or by anybody carrying out a transaction with your consent, regardless of when the transaction is processed to your account.

If you are responsible for a mistaken BPAY payment and we cannot recover the amount from the person who received it within 20 business days of us attempting to do so, you are liable for that payment.

No chargebacks or reversals are provided through the BPAY scheme where you have a dispute with the biller about any goods or services you may have agreed to acquire from the biller, including where the merchant has failed to deliver the goods and services to you.

51.6 Cancellation of access to BPAY

Your access to BPAY is through Phone Banking, Internet Banking or Mobile Banking. BPAY is not severable from these access services. If you wish to cancel your access to BPAY, you will need to cancel your access to Internet Banking (including Mobile Banking) and/or Phone Banking. Similarly, if we to cancel your access to BPAY, we will need to cancel these other services.

Subject to this:

- you may cancel your access to BPAY at any time by giving us written notice;
- we may immediately cancel or suspend your access to BPAY at any time for security reasons, on reasonable grounds, or if you breach these terms and conditions;
- we may cancel your access to BPAY for any reason by giving you 30 days' notice. The notice does not have to specify the reasons for cancellation; and
- if, despite the cancellation of your access to BPAY, you carry out a BPAY payment using the access method, you will remain liable for that BPAY payment.

Your access to BPAY will be terminated when:

- we notify you that your access method or the account with us has been cancelled;
- you close the last of your accounts with us, which has BPAY access;
- you cease to be our member; or
- you alter the authorities governing the use of your account or accounts with BPAY access (for example, you change your account to "all to sign") unless we agree otherwise.

52. Mobile Banking

Mobile Banking is an additional feature of Internet Banking and is not a stand-alone product. You must be registered for Internet Banking before you can use Mobile Banking. To use the Mobile Banking App, you must have a device that is capable of accessing and using the Mobile Banking App. You may download the Mobile Banking App from our website or the relevant App store.

Not all Internet Banking services and features are available from Mobile Banking. We may vary the services we make available and/or which of your accounts may be accessed using Mobile Banking.

For joint accounts that operate on an "any two to sign" or "all to sign" authority, you will not be able to transfer funds or make payment through Mobile Banking.

We do not charge a license fee for the Mobile Banking App. However, you may incur data and/or usage charges from your mobile network when you download and/or use the app. You should check with your service provider that the mobile device will be able to use relevant networks in those countries in which you are travelling.

52.1 Mobile Banking security

Mobile Banking provides the same high-level security and uses the same encryption protocol as Internet Banking, so your personal information and transactions are protected.

The first time that you access the Mobile Banking App, you will be required to enter your member number and Internet Banking password. You must then set a four--digit PIN that will be used to access the service from that point forward. Your PIN cannot be repeated or consecutive numbers or any other easily recognisable code. Your Mobile Banking App PIN should not be the same as the passcode used to access your device.

Remember: to protect your account from unauthorised transactions occurring - where you may not be able to recover the funds- you must NOT use a password that resembles your birth date or part of your name.

When you subsequently access Mobile Banking, if you exceed the allowable number of attempts to login to the Mobile Banking App, your access will be locked and you will need to contact our Member Experience Centre and quote your access code to restore access.

52.2 Biometric identifier

If you have a compatible device and you enable biometric identifier such as fingerprint login in the Mobile Banking App settings, we may permit you to log in to Mobile Banking using the fingerprint(s) that you have registered on that device. On some devices, if you enable the same biometric identifier on the device, you may also be able to log into Mobile Banking using any other passcode that you have established on that device.

If you enable the fingerprint login option, any of the fingerprints stored on your device can be used to log into Mobile Banking. You must ensure that only your fingerprint(s) are stored on the device. We recommend that you establish a passcode to prevent unauthorised access to the device.

When you log into Mobile Banking using the fingerprint login, you instruct us to perform any transactions requested during the Mobile Banking session.

53. Telegraphic transfers

You may use Internet Banking to send funds to an overseas recipient. Under arrangements we have with Convera Australia Pty Ltd ABN 24 150 129 749 and AFSL 404092, telegraphic transfers which you initiate through Internet Banking will be sent to the beneficiary's account via Convera. This facility is provided to you by us. Convera has no responsibility or liability to you for the provision of financial services to you or any loss of any kind whatsoever (including consequential loss and expense) arising in connection with the funds transfer.

You are responsible for the completeness and accuracy of the information you provide for telegraphic transfers. If the information you provide is incorrect, the payment may be rejected or credited to the wrong person (even if that account is not in the name of the stipulated beneficiary). We will not generally be able to recover a payment made in error. We are not liable for any loss you incur as a result of errors or omission in payment details you provide.

If you request a telegraphic transfer through Internet Banking, we will provide you with a quote. Your acceptance of a quote will constitute your instruction and authorisation to us to immediately debit the value of your telegraphic transfer (in Australian dollars) from the account you have nominated when using the facility (including the applicable fees and charges payable to us), and to transfer funds to the account of the beneficiary.

Telegraphic transfers are processed using intermediary banks determined by Convera. The majority of overseas banks levy other processing charges that vary between banks/countries, which may be deducted from the amount received by the beneficiary.

A transaction confirmation issued in Internet Banking does not signify that the telegraphic transfer has been received into the account of the beneficiary.

The overseas bank will normally receive the transfer of funds within 24 hours and, if it is not the beneficiary bank, may take any normal length of time to on forward the funds to the beneficiary's bank.

Subject to the ePayments code, we are not responsible for any delays in transmission or payment and we are not liable for any loss caused by any such delay. We are not liable for any loss as a result of the beneficiary bank's failure or delay, except to the extent that the delay was caused by our negligence or wilful misconduct, in advising the beneficiary of a credit to their account.

54. NPP, PayID, PayTo, NPP International Payments and Osko

We participate in the NPP which enables you to make and receive near real-time payments through your eligible account and to and from anyone at another participating financial institution. This **clause 54** also sets out the terms on which you create and maintain a PayID for receiving NPP Payments, how the PayTo service is provided and the terms on which we will allow you to do so.

Osko is a service provided by BPAY enabling you to make NPP Payments using a PayID or using the BSB and account number of the person or organisation you wish to pay in accordance with this **clause 54**. NPP Payments and Osko Payments are available through Internet Banking, Mobile Banking, or, in restricted cases, through a branch and the Member Experience Centre.

54.1 NPP PayID Terms of Use Making and receiving NPP Payments using PayID

The PayID Service enables payers to make NPP Payments to payees using an alternative identifier instead of account details. 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. This means we may ask you to provide evidence to establish this to our satisfaction irrespective of whether you have registered for any EFT access services with us.

Whether you choose to create a PayID for your account or not, you and each authorised user may use a payee's PayID to make particular types of NPP Payments to the payee from your account provided that:

- we and the payee's financial institution support the NPP Payment service;
- the Payee's account can receive the particular NPP Payment; and
- the PayID is not Locked.

Refer to **clause 55** for the Osko Terms of Use which sets out how a PayID may be used for particular NPP Payment services, your obligations to input correct PayID details and to check the payee's PayID Name before sending an NPP Payment.

Refer to **Part 6** for your rights in relation to the investigation and recovery of mistaken payments, misdirected payments and unauthorised (including fraudulent) NPP Payments.

54.2 Choosing a PayID and PayID Name

The PayID Types we support are limited to your (note that we may update this list from time to time):

- mobile number;
- email address; and
- ABN, ACN, ARBN or ARSN for business members.

You may create a PayID if it is a supported PayID Type. Some PayID Types are restricted to business members and organisations. Only eligible members will be able to request a PayID that is a restricted PayID Type.

Depending on the policy of a payer's financial institution, your PayID Name will be displayed to payers who send NPP Payments to you using your PayID. When you create your PayID, we will enable you to confirm your selection of a PayID Name for display to payers. We do 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 which for any reason is inappropriate.

54.3 Creating your PayID

We will not create a PayID for you without your prior consent.

You may choose to create more than one PayID for your account. For joint accounts, each account holder may create a unique PayID for the account. Each authorised user with full access to the eligible account in Internet Banking may create a unique PayID for the account. However, an authorised user with view-only access to the eligible account in Internet Banking will not be able to register a PayID for the account.

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. See **clause 54.4** for details on transferring PayIDs.

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 PayID Service, you will see the following message "Unable to Register PayID". You can contact our Member Experience Centre to discuss duplicate PayIDs or visit the FAQs on our website creditunionsa.com.au. We cannot disclose details of any personal information in connection with duplicate PayIDs.

54.4 Transferring your PayID to another account

You can transfer your PayID to another account with us or to an account with another financial institution by submitting a request through Internet Banking or Mobile Banking. A transfer of your PayID to another account with us will generally be effective immediately unless we notify you otherwise.

A transfer of your PayID to another financial institution is 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. You can request transfer of your PayID at any time and as often as you wish.

A locked PayID cannot be transferred (see **clause 54.6**).

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 and complete the transfer to us through Internet Banking or Mobile Banking.

54.5 Closing a PayID

You can only close your PayID through Internet Banking or Mobile Banking. You must immediately close your PayID if you no longer own it or have authority to use it.

54.6 Locking and Unlocking a PayID

You can lock your PayID through Internet Banking or Mobile Banking. If you locked the PayID, you can unlock it through Internet Banking or Mobile Banking.

We monitor PayID use to manage PayID misuse and fraud. You acknowledge and consent to us locking your PayID if we reasonably suspect misuse of your PayID or use of your PayID to procure NPP Payments fraudulently. If we locked the PayID, you can request us to unlock it by contacting our Member Experience Centre or visiting a branch.

54.7 NPP Payments

We will ensure that your PayID and account details are accurately recorded in the PayID Service. Where we and the sending financial institution determine that an NPP Payment made to your account is either a mistaken payment or 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 (see **clause 62**).

54.8 NPP International Payments

An NPP International Payment received from overseas through the NPP will be paid to your eligible account and will appear on your statement as "NPP International Payment.".

NPP International Payments originated in a foreign currency will be converted to Australian dollars.

54.9 Privacy

By creating your PayID you acknowledge that you authorise:

- us to record your PayID Record in the PayID service;
- NPP participants which are payers' financial institutions to use your PayID information for the purposes of constructing NPP payment messages, enabling payers to make NPP Payments to you, and to disclose your PayID Name to payers for NPP Payment validation.

To the extent that the creation and use of the PayID Record constitutes disclosure, storage and use of your personal information within the meaning of the Privacy Act, you acknowledge and agree that you consent to that disclosure, storage and use.

54.10 PayTo Terms of Use

PayTo allows us to receive and authorise, PayTo Agreements created at your request with Merchants or Payment Initiators who offer PayTo as a payment option.

With PayTo you can create, amend, pause and cancel PayTo Agreements.

You can use PayTo through our Internet Banking service and our Mobile Banking App.

54.10.1 Creating a PayTo Agreement

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

PayTo Agreements must be recorded in the Mandate Management Service in order for NPP Payments to be processed in accordance with them. The Merchant or Payment Initiator is responsible for creating and submitting a record of each PayTo Agreement to their financial institution or payments processor for inclusion in the Mandate Management Service. The Mandate Management Service will notify us of the creation of any PayTo Agreement established using your Account or PayID details. We will deliver a notification of the creation of the PayTo Agreement to you via our Mobile Banking App and Internet Banking and provide details of the Merchant or Payment Initiator named in the PayTo Agreement, the payment amount (if provided) and payment frequency to seek your confirmation of the PayTo Agreement. You may authorise or decline any PayTo Agreement presented for your approval. If you authorise, we will record your authorisation against the record of the PayTo Agreement in the Mandate Management Service and the PayTo Agreement will then be deemed to be "active". If you decline, we will note that against the record of the PayTo Agreement in the Mandate Management Service and the status will be set to "cancelled".

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

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

If you believe the payment amount or frequency or other details are presented incorrectly, you may decline the PayTo Agreement and contact the Merchant or Payment Initiator and have them amend and resubmit the PayTo Agreement creation request.

54.10.2 Amending a PayTo Agreement

From time to time, your PayTo Agreement may be amended by the Merchant or Payment Initiator, you or us on your instruction.

We will send you notification of proposed amendments to the payment terms of the PayTo Agreement requested by the Merchant or Payment Initiator. Such amendments may include variation of the payment amount, where that is specified in the PayTo Agreement as a fixed amount, or payment frequency. The Mandate Management Service will notify us of the amendment request. We will deliver a notification of the proposed amendment to you via our Mobile Banking App and Internet Banking for your approval. You may confirm or decline any amendment request presented for your approval. If you confirm, we will record the confirmation against the record of the PayTo Agreement in the Mandate Management Service and the amendment will then be deemed to be effective. If you decline, the amendment will not be made. A declined amendment request will not otherwise affect the PayTo Agreement.

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

If you decline the amendment request because it does not reflect the updated terms of the agreement that you have with the Merchant or Payment Initiator, you may contact them and

have them resubmit the amendment request with the correct details. We are not authorised to vary the details in an amendment request submitted by the Merchant or Payment Initiator.

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

Once a PayTo Agreement has been established, you may amend or instruct us to do it, to update your name or Account details in the PayTo Agreement only. Account details may only be replaced with the BSB and account number or with the PayID of an account you hold with us. We may decline to act on your instruction to amend your PayTo Agreement if we are not reasonably satisfied that your request is legitimate. You may not request us to amend the details of the Merchant or Payment Initiator, or another party.

54.10.3 Pausing your PayTo Agreement

You may instruct us to pause and resume your PayTo Agreement by sending us a Secure Mail message via your Internet Banking or by contacting our Member Experience Centre. We will act on your instruction to pause or resume your PayTo Agreement promptly by updating the record of the PayTo Agreement in the Mandate Management Service. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption. During the period the PayTo Agreement is paused, we will not process payment instructions in connection with it. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a PayTo Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator.

Merchants and Payment Initiators may pause and resume their PayTo Agreements. If the Merchant or Payment Initiator pauses a PayTo Agreement to which you are a party, we will promptly notify you of that, and of any subsequent resumption, via our Mobile Banking App or Internet Banking. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a PayTo Agreement by the Merchant or Payment Initiator.

54.10.4 Cancelling your PayTo Agreement

You may instruct us to cancel a PayTo Agreement on your behalf by sending us a Secure Mail message via your Internet Banking or by contacting our Member Experience Centre. We will act on your instruction promptly by updating the record of the PayTo Agreement in the Mandate Management Service. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the cancellation. You will be liable for any loss that you suffer as a result of the cancellation of a PayTo Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator (for example, any termination notice periods or fees that have not been adhered to). Merchants and Payment Initiators may cancel PayTo Agreements. If the Merchant or Payment Initiator cancels a PayTo Agreement to which you are a party, we will promptly update the record of the PayTo Agreement to a "cancelled" status in the Mandate Management Service. We will not be liable to you or any other person for loss incurred as a result of cancellation of your PayTo Agreement by the Merchant or Payment Initiator.

54.10.5 Migration of DDR arrangements

Merchants and Payment Initiators who have existing direct debit arrangements with their customers, may establish PayTo Agreements for these, as Migrated DDR PayTo Agreements, in order to process payments under those arrangements via the NPP. If you have an existing DDR arrangement with a Merchant or Payment Initiator, you may be notified by them that future payments will be processed from your Account through PayTo. You are entitled to prior written notice of variation of your DDR arrangement and changed processing arrangements, as specified in your direct debit service agreement, from the Merchant or Payment Initiator. If you do not consent to the variation of the DDR arrangement you must advise the Merchant or Payment Initiator. We are not obliged to provide notice of a Migrated DDR PayTo Agreements to you for you to confirm or decline. We will process instructions received from a Merchant or Payment Initiator on the basis of a Migrated DDR PayTo Agreement.

You may amend, pause (and resume) or cancel your Migrated DDR PayTo Agreement, or receive notice of amendment, pause or resumption, or cancellation initiated by the Merchant or Payment Initiator, in the manner described in clauses 54.10.2, 54.10.3 and 54.10.4.

54.10.6 Your responsibilities for PayTo Agreements

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

You must notify us immediately if you no longer hold or have authority to operate the Account from which payments under a PayTo Agreement or Migrated DDR PayTo Agreement have been or will be made.

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

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

You are responsible for ensuring that you have sufficient funds in your Account to meet the requirements of all your PayTo Agreements and Migrated DDR PayTo Agreement. Subject to any applicable laws and binding industry codes, we will not be responsible for any loss that you suffer as a result of your Account having insufficient funds. These terms and conditions will apply in relation to circumstances where there are insufficient funds in your Account.

If you receive a PayTo Agreement creation request or become aware of payments being processed from your Account that you are not expecting, or experience any other activity that appears suspicious or erroneous, please report such activity to us by sending us a Secure Mail message via your Internet Banking or by contacting our Member Experience Centre immediately.

If you use a mobile device to do your banking, we recommend that you allow notifications from our Mobile Banking App to your device to ensure that you are able to receive and respond to PayTo Agreement creation requests, amendment requests and other notifications in a timely way.

Use of the facilities that we provide to you in connection with establishing and managing your PayTo Agreements and Migrated DDR PayTo Agreements is required to meet terms and conditions for their use which are available on our website www.creditunionsa.com.au or by calling the Member Experience Centre.

You are responsible for ensuring that:

• all data you provide to us or to any Merchant or Payment Initiator that subscribes to the PayTo service is accurate and up to date;

• you do not use the PayTo service to send threatening, harassing or offensive messages to the Merchant, Payment Initiator or any other person; and

• any passcode needed to access the facilities we provide are kept confidential and are not disclosed to any other person.

54.10.7 Our responsibilities

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

We may monitor your PayTo Agreements or Migrated DDR PayTo Agreements for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your PayTo Agreement or Migrated DDR PayTo Agreements if we reasonably suspect misuse, fraud or security issues. We will

promptly notify you by sending you a message through our Mobile Banking App or Internet Banking of any such action to pause or cancel your PayTo Agreement.

If you become aware of a payment being made from your Account, that is not permitted under the terms of your PayTo Agreement or Migrated DDR PayTo Agreement or that was not authorised by you, please contact us as soon as possible by sending us a Secure Mail message via your Internet Banking or by contacting our Member Experience Centre and submit a claim. We will respond to all claims within five business days of receiving your claim and if the claim is founded, we will refund your Account. We will not be liable to you for any payment made that was in fact authorised by the terms of your PayTo Agreement or Migrated DDR PayTo Agreement.

54.10.8 Privacy

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

55. Osko Terms of Use

We subscribe to the Osko Scheme and offer the Osko Payments service (called Service 1 by BPAY) which allows Members to make and receive Osko Payments in near real-time. Osko Payments can be made using Internet Banking or Mobile Banking. Osko transactions are identified by the Osko logo.

Notifications to you about Osko Payments will be displayed on screen for you to confirm with an on-screen receipt confirming when the payer financial institution accepts the payment instruction.

We will notify you if, for any reason, we are no longer able to offer you Osko. If we are no longer able to offer you Osko, you will not be able to send or receive Osko Payments through us.

Where we are able to do so, we will notify you:

- if there are any delays in processing Osko Payments;
- when your Osko Payment is likely to be completed; and
- give you the opportunity to cancel an Osko Payment if it is delayed.

55.1 How to use Osko

The eligible accounts for linking to Osko Payments are set out in **Table** in **clause 19**. You use the same payment procedures used for Internet Banking and Mobile Banking with the additional requirements for Osko Payments set out in this clause.

55.2 How Osko Payments work

Osko Payments must be single immediate payments.

55.3 Payment Directions

You must give us the information specified in this **clause 55.3** when you send us a payment direction. Subject to applicable laws, including where applicable the ePayments Code, we will treat your instruction to make an Osko Payment as valid if you provide us with the following information:

- the amount of the Osko Payment; and
- if you elect:
  - not to use PayID, the details of the BSB and account number of the Payee's account to be credited with the amount of the Osko Payment; or
  - to use PayID, the Payee's PayID

You should ensure that all information you provide in relation to an Osko Payment is correct. We will not be able to cancel an Osko Payment once it has been processed.

56. Cancellation of access services

56.1 When you may cancel your access services

You may request to cancel any access services by contacting Member Experience Centre and quoting your access code, by visiting a branch or, where permitted for the type of account, using Internet Banking, Mobile Banking or through your digital wallet.

56.2 When we may cancel or suspend your access to access services

We may cancel or suspend any access service at any time:

- you cease to be a member;
- you close your accounts;
- if we consider, on reasonable grounds, that it is necessary or desirable to protect our security and/or the security of your accounts, including where we suspect your account or access method has been compromised or is at risk of being compromised;
- where we suspect, on reasonable grounds, that you or an authorised user is acting fraudulently;
- if we suspect, on reasonable grounds, that you are using the access service that will or is likely to affect our ability to continue providing the access service to you or our other members or customers of other financial institutions;
- if you breach any material obligation under these terms and conditions which is capable of remedy and do not remedy that breach within 20 business days of receiving a notice from us specifying the breach and requiring the breach to be remedied;
- you breach any material obligation under these terms and conditions which is incapable of remedy;
- if you suffer an insolvency event;
- you or a joint account holder becomes deceased if we consider, on reasonable grounds, that it is necessary; or
- your account becomes dormant; or
- in the case of Internet Banking, BPAY or Osko, our participation in NPP or membership to the BPAY scheme or subscription to Osko is suspended, ceased or cancelled for any reason.

Termination or suspension of your right to use Osko does not:

- prejudice any claims either party may have against the other in respect of any then subsisting breaches of these terms and conditions; or
- otherwise affect the accrued rights or remedies of either party.

57. Foreign Currency Purchase

You may call the Member Experience Centre or come into the branch to purchase foreign currency. Credit Union SA arranges for the sale and repurchase of foreign cash in conjunction with Travelex. The minimum cash order per currency is the equivalent of AUD250. The exchange rates are updated on a daily basis and are subject to change throughout the day. For details on fees and charges refer to BRC 1004 Deposit Accounts Fees and Charges brochure.

Foreign currency can be purchased via a link on the Credit Union SA website. You are responsible for the completeness and accuracy of the information that you supply to Travelex through the Credit Union SA website.

Orders placed with an employee prior to 2.00pm are available for collection by

the member on the third working day after the order is placed. Orders placed on-line after 2.00pm are available for collection by the Member on the fourth working day after ordering.

Foreign currency can only be repurchased from a member attending the branch in person.

The minimum repurchase amount Credit Union SA can accept is AUD1,000.

Part 5
Security and liability for unauthorised transactions

58. Guidelines for safeguarding your codes

You must protect the security of your passcodes as a means of preventing fraudulent or unauthorised use of an access method. You must take care to ensure that access methods are not lost or stolen and that your passcodes do not become known to anyone else.

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 these terms and conditions and the ePayments Code.

We will never ask you to disclose your PIN or passcode to us, other than your Access Code – refer **clause 38** (Access Code).

58.1 How to protect your passcode?

- **Do not use a passcode that represents your birthday, postcode or a recognisable part of your name or address.** If you do use an obvious passcode, you may be liable for any losses that occur as a result of unauthorised use of the passcode before you notify us that the passcode has been misused or become known to someone else.
- Do not tell or show your passcode to another person (including family member or friend).
- Do not allow anyone to see you enter your passcode into a device or hear you provide your passcode.
- Do not leave a device unattended and logged into an access method.
- Where a device is needed to perform a transaction, do not write or record your passcode on the device and/or do not keep a record of the passcode on anything that is carried with the device or liable to loss or theft simultaneously with the device unless you make a reasonable attempt to disguise the passcode.
- Where a device is not needed to perform a transaction, do not keep a written record of all passcodes 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 passcodes.
- Change your passcode regularly.
- If you suspect that someone else may know your passcode or that an unauthorised person is using your passcode, you should change your passcode immediately and contact us.

58.2 What is a reasonable attempt to protect your passcode?

If you keep a written record of your passcode, you must take reasonable steps to disguise the passcode. What is reasonable will depend on the facts in each instance, but includes any reasonable attempt to disguise the passcode within the record or prevent unauthorised access to the record, including:

- hiding or disguising the passcode record among other records;
- hiding or disguising the passcode record in a place where such a record would not be expected to be found;
- keeping the passcode record in a securely locked place; or
- preventing unauthorised access to an electronically stored record of the passcode.

59. Guidelines for safeguarding your card and account details

The following guidelines are in addition to the guidelines set in **clause 58.**

59.1 How to protect your card and account details?

- When you receive a new card and PIN (or replacement card or PIN), we will advise you on the steps you need to take to activate your card. You will need to do this before being able to use your card.
- Keep your member number, account numbers and card details as confidential.
- Sign your card immediately upon receiving it and before using it.
- Carry your card whenever possible.
- Keep your card in a safe secure place and check regularly to ensure that your card is not lost or stolen.
- Never lend your card to another person (including family members and friends).
- Only disclose your card and/or account details to a third party when there is a reasonable need to do so. For example, where you ask someone to transfer funds to your account electronically, or where you authorise a direct debit or where you purchase goods online or over the phone.

60. Guidelines for protecting your devices and digital wallets

The following guidelines are in addition to the guidelines set out in **clause 58.**

60.1 How to protect your device and digital wallet?

- Where your device can be accessed by a biometric identifier such as fingerprint login, ensure only your biometric identifier is registered on that device.
- If another person's biometric identified is loaded onto your device, take steps to remove that person's biometric identifier before you transact using your device.
- Ensure that your device is locked at all times when it is not being used and is not left unattended in a non-secure environment.
- Install and regularly update anti-virus software on your device.
- Ensure that only you have access to your digital wallet to use your card. Do not allow another person to access your digital wallet (including family members and friends).
- Remove any card from your device before you dispose of your device.
- Do not lend your device to anyone or permit another person (including family members) to use the device.

61. Reporting loss, theft or unauthorised use of card, PIN or device containing a digital wallet

If you believe that a card, a PIN or a device containing a digital wallet has been lost, stolen, become known to another person or otherwise used without your authority, you must immediately report the incident as follows depending on whether you are in Australia or overseas.

Please note that we do not have control over any charges applied by the local or international telephone company for contacting us.

We will accept a report of an unauthorised transaction provided you submit the report to us within the timeframe included in the ePayments Code, from the day you first become aware of the unauthorised transaction.

61.1 If you're in Australia

Choose one of the following methods to report the incident to us:

- Log in to your Mobile Banking App and go to the ***Card management*** menu item. Select your card from your card list and then ***Lost or Stolen card***. Select from either ***Lost card*** or ***Stolen card*** and follow the onscreen instructions to cancel it.
- Log in to your Internet Banking and select ***Cards > Card management*** and select ***Report card lost/stolen***.
- Call our Member Centre **(08) 8202 7777** (during business hours) or the 24-Hour card hotline on 1800 648 027 (if after hours) to notify us of your lost or stolen card.

61.2 If you're overseas

Choose one of the following methods to report the incident to us:

- Log in to the Mobile Banking App and go to the ***Card management*** menu item. Select your card from your card list and then ***Lost or Stolen card***. Select from either ***Lost card*** or ***Stolen card*** and follow the onscreen instructions to cancel it.

- Log in to your Internet Banking and select ***Cards > Card management*** and select ***Report card lost/stolen***.
- Call **+612 8299 9101** to cancel your card.

61.3 If you are overseas and need a replacement card

Choose one of the following methods to request a replacement card:

- Call us on **+618 8202 7777** (access code required) during business hours to request a replacement card;
- Send us a Secure Mail message via your Internet Banking with your request and current location for delivery of your replacement card;
- Send us a signed fax on **+61 8 8211 9457** with your request and current location for delivery of your replacement card.

61.4 How we investigate the incident about your card, PIN or digital wallet

We or the card hotline will acknowledge your report by giving you a reference number. You should keep this reference number as proof of the date and time that you reported the incident. You must provide the card number, the name of your credit union (if reporting to the card hotline) and any other personal information you are asked to provide to assist in identifying you and/or the compromised card.

If for any reason the card hotline is unavailable and this prevents you from reporting the incident, you will not be liable for any unauthorised transaction which could have been prevented during the period if the card hotline had been available, provided that we are notified as soon as practicable after the card hotline becoming available again.

Where appropriate, we will reset your passcode, stop your card and/or prevent transactions from being performed using that access method until a new passcode and/or card has been issued.

If the loss, theft or misuse of a card occurs outside Australia, you can confirm the loss, theft or misuse of the card:

- with us by telephone or priority paid mail as soon as possible; or
- by contacting the Visa Worldwide card hotline number for the country you are in (you can obtain this number from us prior to your departure).

62. Mistaken internet payment

You can be either the sender of a mistaken internet payment or the receiver of a mistaken internet payment.

When making a payment through Internet Banking (such as auto transfers or NPP Payments), you should take care to ascertain that the BSB number, account number and/or identifier such as PayID you have entered are correct, because payments are processed using these details and without checking the account name. It may not be possible to recover funds from an unintended recipient.

We will not charge you a fee for contacting us.

62.1 How we handle mistaken internet payments

You must report a mistaken payment as soon as possible. We will acknowledge your report and investigate whether a mistaken internet payment has occurred. If we are satisfied that a mistaken internet payment has occurred, we will send the receiving ADI a request for the return of the funds as soon as reasonably possible and no later than 5 business days from the time you submitted your report of a mistaken internet payment. If we are not satisfied that a mistaken internet payment has occurred, we are not required to take any action.

If the mistaken internet payment was made to an unintended recipient account held with us, we will return to you any funds we retrieve from the unintended recipient. The process is set out in **clause 62.2**.

If a mistaken internet payment has been made to an unintended recipient held with another ADI, we will return you any funds the receiving ADI provides to us as soon as practicable. The process is set out in **clause 62.3**. If the receiving ADI does not agree that a mistaken internet payment has occurred, it may (but is not obliged to) ask the consent of the unintended recipient to return the funds. If the unintended recipient agrees to return the funds, the receiving ADI must return the funds.

62.2 Unintended recipient's account is held with us

If we have determined that a mistaken internet payment has been made to an unintended recipient whose account is held with us, then:

- If the account into which the mistaken internet payment was made does not have sufficient credit funds to the full value of the mistaken internet payment, we will use reasonable endeavours to retrieve the funds from the recipient for return to you.
- If the account into which the mistaken internet payment was made does have sufficient credit funds to the full value, then the following applies:
  - (a) where the report is made within 10 business days, we will return the funds to you within 5 business days of determining that the payment is a mistaken internet payment if practicable, although we may reasonably delay the payment up to a maximum of 10 business days.
  - (b) where report is made between 10 business days and 7 months, we will give the unintended recipient 10 business days to establish that it is entitled to the funds. If it does not do so, we will return the funds to you within 2 business after the expiry of that period.
  - (c) where the report is made after 7 months, we will ask the unintended recipient if it agrees to the return of the funds to you. If it agrees, we will return the funds to you as soon as practicable.

Despite the above, if the unintended recipient is receiving income support payments from Services Australia or Department of Veterans' Affairs payments we will recover the funds from the recipient in accordance with the Code of Operation: Recovery of debts from customer nominated bank accounts in receipt of Services Australia income support payments or Department of Veterans' Affairs payments.

62.3 Unintended recipient's account is held with a receiving ADI

If we have determined that a mistaken internet payment has been made to an unintended recipient whose account is held with a receiving ADI, we will adhere to the ePayments Code process to attempt to retrieve your funds as follows:

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

When you report a mistaken internet payment within 10 business days of making the payment and:

- we and the receiving ADI are satisfied that a mistaken internet payment has occurred; and
- we are advised by the receiving ADI that there are sufficient credit funds available in the account of the unintended recipient to the value of the mistaken internet payment,

the receiving ADI must forward the funds to us no later than 10 business days after receiving our request to return the funds unless the payment was an NPP Payment, in which case the receiving ADI may return the funds.

Process where funds are available and the report is made after 10 business days and 7 months

When you report a mistaken internet payment between 10 business days and seven months after making the payment and:

- we and the receiving ADI are satisfied that a mistaken internet payment has occurred; and

- we are advised by the receiving ADI that there are sufficient credit funds available in the account of the unintended recipient to the value of the mistaken internet payment; and
- the receiving ADI prevents the unintended recipient from withdrawing the funds for 10 business days and during this period the unintended recipient does not establish they it is entitled to the funds, then

the receiving ADI must forward the funds to us within 2 business days after the expiry of the 10-business day period referred to above. Unless the payment was an NPP Payment, the funds must be forwarded to us within 2 business days of the expiry of this period.

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

When the report of the mistaken internet payment is made more than 7 months after making the payment and:

- we and the receiving ADI are satisfied that a mistaken internet payment has occurred; and
- we are advised by the receiving ADI that there are sufficient credit funds available in the account of the unintended recipient to the value of the mistaken internet payment; and
- the unintended recipient consents to return of the funds,

the receiving ADI must forward the funds to us unless the payment was processed through the NPP or OSKO in which case the receiving ADI may return the funds.

Where the unintended recipient of a mistaken internet payment is receiving income support payments from Services Australia or Department of Veterans' Affairs payments, the receiving ADI must recover the funds from the unintended recipient in accordance with the Code of Operation: Recovery of debts from customer nominated bank accounts in receipt of Services Australia income support payments or Department of Veterans' Affairs payments.

Process where the funds are not available

Where we and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are insufficient 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 endeavors to retrieve the funds from the unintended recipient in order to return the funds to you. The receiving ADI must exercise discretion, based on an appropriate weighing of interests of both the payment sender and unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should:

- pursue the return of funds to the total value of the mistaken internet payment,
- pursue the return of funds representing only a partial amount of the total value of the mistaken internet payment, or
- not pursue any return of funds (whether partial or total).

If the receiving ADI is unable to retrieve the funds from the unintended recipient, you will be liable for losses arising from the mistaken internet payment.

62.4 Where you are the unintended recipient

If you are an unintended recipient, you authorise us to withdraw the funds from your account without giving you advance notice and return the funds to the sending ADI in order for us to comply with the requirements of the ePayments code.

62.5 If you have a complaint about mistaken internet payments and misdirected payments

We must inform you in writing of the outcome of your reported mistaken internet payment, within 30 business days of the day on which your report is made.

If you are not satisfied with how your report about a mistaken internet payment was handled by us or the receiving ADI or the outcome of your report, you can lodge a complaint with us. See **Part 6** on how to lodge a complaint and how we handle complaints.

63. Liability for unauthorised EFT transactions

63.1 When you are not liable for EFT transactions

You will not be liable for losses to your account from an unauthorised EFT transaction if the cause of the loss is any of the following:

- fraudulent or negligent conduct of our employees or agents, or the employees or agents of any other organisation involved in the provision of that access method, or any merchant or their employee or agent;
- a device, identifier or passcode which is forged, faulty, expired or cancelled;
- a transaction requiring the use of a device and/or passcode that occurred before you received the device and/or passcode (including a reissued device and/or passcode);
- an unauthorised transaction performed after you notify us that a device has been misused, lost or stolen, or the security of a passcode has been breached;
- a transaction being debited more than once to your account (you will not be liable in such cases even if there has not been unauthorised access); or
- where your correct membership number and/or passcode have not been used to access your account via the designated access method.

A mistaken internet payment is not the same as an unauthorised transaction. For mistaken internet payments, see **clause 62**.

You will not be liable for any loss that would exceed the amount of your liability to us if we had exercised our rights (if any) under the Visa Worldwide Rules and Regulations against other parties to those rules and regulations.

64. Other unintended receipt of funds

64.1 Where you are the unintended recipient

If we are reasonably satisfied that funds have been paid into your account due to another party's mistake, unauthorised activity or fraud, we may, without prior notice to you, debit any credit balance in your account (on more than one occasion if necessary) to repay the other party.

64.2 When you are liable for EFT transactions

You will be liable for losses to your account from unauthorised access if the losses occur before you notify us that your access method or a card forming part of an access method has been misused, lost, stolen or used without your authority and if we prove, on the balance of probabilities, that you contributed to the loss through:

- your fraud, or your failure to keep your passcode, account and devices secure (refer to requirements of **clauses 58 to 60** for the minimum standard of care that you must exercise); or
- unreasonably delaying in notifying us or the card hotline of the misuse, loss, theft or unauthorised use of your access method or a card or PIN forming part of an access method in accordance with the requirements of **clauses 58 to 60**, and the losses occur between the time you did, or reasonably should have, become aware of these matters and the time of notification to us.

If we decide that you are liable for all or any part of a loss arising out of unauthorised use of an access method or a card forming part of an access method, we will:

- give you copies of any documents or other evidence we relied upon in reaching this decision; and
- advise you in writing whether or not there was any system or equipment malfunction at the time of the relevant transaction.

However, you will not be liable for:

- the portion of the loss that exceeds any applicable daily or periodic transaction limits;

- the portion of the loss on your account which exceeds the balance of your account (including any pre-arranged credit); or
- all losses incurred on any account that you had not agreed with us could be accessed using the access method or a card forming part of an access method.

64.3 When your liability for EFT transactions is limited

Where a transaction is performed using an access method and we are unable to prove on the balance of probabilities that you contributed to the loss, your liability will be the lesser of:

- $150;
- the balance of your account, including any pre-arranged credit; and
- the actual loss at the time you notify us or the card hotline that your access method or a card or PIN forming part of an access method has been misused, lost, stolen or used without your authority (except that portion of the loss that exceeds any applicable daily or periodic transaction limits).

Notwithstanding any other provision in this **clause 64** your liability will not exceed your liability under the ePayments Code.

64.4 What is your liability for other unauthorised transactions?

If, in cases not involving EFT transactions, the card or PIN is used without authority, you are liable for that use before notification to us or the card hotline of the unauthorised use, up to your current daily withdrawal limit.

64.5 When the electronic banking system or EFT terminal breaks down

You will not be responsible for any loss you suffer because the access method accepted your instruction but failed to complete the transaction. If there is a breakdown or interruption to an access method and you were aware or should have been aware that the system was unavailable for use or malfunctioning, we will only be responsible for correcting errors in your account and refunding fees or charges imposed on you as a result.

65. Indemnity

Subject to **clause 64** and the ePayments code, we are not liable for any consequential loss you suffer as a result of using an access method, other than loss due to our negligence or wilful misconduct, 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. You indemnify us against any loss we may incur due to any claim, demand or action of any kind brought against us arising directly or indirectly, except to the extent that the loss was caused by our negligence or wilful misconduct.

Part 6
Resolving disputes

66. Handling complaints

If you have a complaint related to our products or services, please let us know. You can do this through multiple channels including in person, telephone, online, social media and email or letter to:

Credit Union SA Dispute Resolution Officer

Email: info@creditunionsa.com.au
(attention Dispute Resolution Officer)

Post: GPO Box 699 Adelaide SA 5001

We will try to resolve your complaint as soon as possible ("on the spot"). Rest assured we will do everything we can to resolve it to your satisfaction.

If we are not able to resolve your complaint immediately, we will acknowledge and investigate your complaint providing you with an update on its progress within 3 business days of receiving it.

If we are able to resolve your complaint within five business days of receiving it, we will only provide you with a written response on your request.

If we are unable to resolve your complaint within five business days of receiving your complaint, we will advise you of the procedures for further investigation and may ask you to provide further information.

We will do our best to ensure that our investigation is completed within 21 days of receiving your complaint. However, in some cases it may take up to 30 days if we need more information to assess your complaint or if your complaint is complex. We will notify you in writing of either the outcome of our investigation or the fact that we require more time to complete our investigation (timeframe depends on what your complaint is about). We will provide regular progress updates.

We will complete our investigation within 45 days of receiving your complaint, unless there are exceptional circumstances. In such circumstances, we will let you know the reasons for the delay and provide you with monthly updates on the progress of the investigation and its likely resolution date, except where we are waiting for a response from you and you have been advised that we require such a response.

67. Handling disputed transactions and mistaken payments

You should carefully check all entries on your account statements. If you believe that a transaction or payment of any type was not authorised by you or has not been processed correctly, you should contact us at:

Member Experience Centre

During business hours:
(08) 8202 777 or
1800 018 227 (in country SA)

or

Other times:
08 8202 7634

We will notify you of the steps you must take so we can investigate the disputed transaction. You must give us full details of the transaction you are disputing.

68. Outcome of our investigation

When we complete our investigation of your complaint, we will notify you of:

- the result of our investigation;
- reasons for our decision, including reference to the relevant clauses of these terms and conditions or the ePayments Code (if applicable) or the code of practice; and
- any further action that you may take in respect of your complaint

However, we are not obliged to provide you with reasons if we are able to resolve your complaint within five business days from receiving it, unless you request us to do so.

If we found that an error was made, we will make the appropriate adjustment to your affected account (including any interest and charges) and notify you in writing of the amount of the adjustment.

If we found that you are liable for all or part of the disputed transaction, we will supply you with copies of any document or other evidence on which we have based our findings if these show that your affected account has not been incorrectly charged or credited. We will notify you in writing if there was any system or equipment malfunction at the time of the transaction.

69. If you are not satisfied with our investigation

The Australian Financial Complaints Authority (AFCA) is a 100% independent, impartial and free service for individuals and small business members.
You can contact AFCA as follows:

Phone: 1800 931 678

Email: info@afca.org.au

Website: www.afca.org.au

Post: GPO Box 3 Melbourne VIC 3001

If your complaint remains unresolved after 45 days (even if we are still investigating your complaint), you can refer your complaint (at no cost to you) to AFCA. We will notify you that you have this right within 5 business days after the end of the 45-day period.

When we notify you of our determination, we will also notify you of further action you may take in respect of your complaint if you are not satisfied with our determination. You may, for instance, refer the matter to AFCA.

70. If we fail to comply with this procedure

If we fail to observe the procedure set out in this **Part 6** of this document and the ePayments Code or the code of practice for handling disputes, allocating liability and communicating the reasons for our determination and that failure contributes to our decision or delays the resolution of your complaint, we may be liable for part of all of the amount of the transaction subject of your complaint.

Want to know more about Credit Union SA or any of our products or services?
We'd be delighted to help.

Visit our website
creditunionsa.com.au

Call us on
(08) 8202 7777

Visit us at
400 King William St, Adelaide SA 5000

Have a Mobile Lending Manager visit you

Credit Union SA Ltd
ABN 36 087 651 232
AFSL/Australian Credit Licence 241066

Credit Union SA Centre
Level 3, 400 King William Street,
Adelaide SA 5000
GPO Box 699 Adelaide SA 5001

BRC_1095 20240429