FSCU

General
Terms and Conditions

Effective 27 November 2025

Contents

Introduction

This Terms and Conditions document provides information about the range of savings accounts, fixed term deposits, and access facilities that Fire Service Credit Union Ltd. (FSCU) offers our members, and sets out the terms and conditions that apply to those accounts, deposits and facilities. It will help you decide whether our products are appropriate for you before you acquire them.

Please read these Terms and Conditions carefully and contact us should you have any enquiries. You should also retain a copy of these Terms and Conditions, but they can also be accessed on our website at www.fscu.com.au or a copy can be obtained from our Office.

These Terms and Conditions should be read in conjunction with our 'Fees and Charges' brochure and our 'Deposit Accounts Interest Rates and Summary of Accounts' document, which form part of the terms and conditions that apply to the accounts, deposits and facilities.

Definitions and Interpretations

In these Terms and Conditions:

Access card means an ATM card, debit card or credit card and includes our Visa Card.

Access Code means a four digit passcode for identification purposes which enables us to verify your identity over the phone.

Access Facility means the facilities we provide to you from time to time to access your accounts in accordance with these Terms & Conditions.

Account means a deposit account with us.

ATM means an automatic teller machine.

Authorised User means you and any person you have authorised to operate your Account.

BPAY means a payment transacted through BPAY to make bill payments to billers who participate in BPAY, either in branch, internet, or any other access method. BPAY® Registered to BPAY Pty Ltd ABN 69 079 137 518.

BSB means a Bank State Branch Number, which identifies the branch of a financial institution in Australia. Our BSB is 805-013.

Business Day means a day that is not a Saturday, Sunday or public holiday or bank holiday in the place concerned.

Card means a debit card or credit card issued by us that can be used to access an Account.

Card Controls means the control functions available for any access card which is not expired, blocked, suspended or cancelled.

Card Details means the information provided on a Card and includes, but is not limited to, the Card number and expiry date.

Card Hotline means the facility made available to you to report of a lost or stolen Card. The card hotline is

1800 648 027.

Chargeback means that, subject to Card scheme rules, we may have a right to return a disputed transaction to a merchant with whom the transaction was made

Complaint means an expression of dissatisfaction made to or about us, related to our products, services or staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.

Contactless means the transaction (such as a Payment) is, will be or has been conducted by holding or tapping a Card or Device (which is capable of making a Contactless transaction) in front of or near an EFT Terminal without having to insert or swipe a Card (e.g. Visa payWave).

Contactless Enabled Card means any Card which is capable of making Contactless transactions.

Contactless Enabled Mobile Device means a mobile device (such as a mobile phone) on which a compatible Contactless Enabled Card has been registered to make Contactless Payments, such as in a Digital Wallet.

Cut Off Time means the time, as we advise you from time to time, by which your payment instructions must be received by us in order for these instructions to be processed that day by BPAY or to allow for transmission to an external party (currently 4pm each Business Day, Monday to Friday).

Days means calendar days, unless otherwise specified.

Device means a device we give to a user that is used to perform a transaction. Examples include: Cards, tokens issued by us that generate a passcode, contactless devices.

Digital Wallet means a software application installed on a compatible Device that allows you to register certain types of Contactless Enabled Cards on the Device to make Contactless Payments using the Device instead of the Contactless Enabled Card (e.g. Google Pay, Apple Pay and Samsung Pay).

Direct entry means a direct debit or direct credit.

EFT Terminal means the electronic equipment, electronic system, communications system or software that we, our agents or any Third Party control or provide for use with an Access Method to conduct an EFT Transaction and includes, but is not limited to, an automatic teller machine or point of sale terminal.

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

Electronic Transaction means any payment, funds transfer or cash withdrawal transaction that is initiated using electronic equipment and not intended to be authenticated by a manual signature.

Facility means an arrangement through which a person can perform transactions (e.g. an account).

Identifier means information that a user knows but is not required to keep secret and must provide to perform a transaction, such as account number.

Migrated DDR Mandates means the PayTo agreement database as maintained by NPP Australia Limited.

Misdirected Payment means a NPP Payment erroneously credited to the wrong account because of an error in relation to the recording of the PayID or associated account information in the PayID service.

Mistaken Internet Payment means a payment by a user through a pay anyone banking facility and processed where funds are paid into the account of an unintended recipient because the user enters or selects a BSB number and/or identifier that does not belong to the named and/or intended recipient

NPP means New Payments Platform operated by NPP Australia Limited.

NPP Payments means payments cleared and settled via the NPP.

Osko means the Osko Payment service provided by BPAY

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

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

Participating online Merchant means a retailer or Merchant who offers goods or services for sale online, who is a participant in Verified by Visa.

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

- Personal identification number (PIN)
- Internet banking passcode
- Code generated by a physical security token
- Code provided to a user by SMS, email or in a mobile application

A passcode does not include a number printed on a device (e.g. a security number printed on a credit or debit card).

Pay anyone banking facility means a facility where a user can make a payment from one bank account to a third party's bank account by entering, selecting or using a Bank/State/Branch (BSB) and account number or other identifier, but does not include BPAY or PayTo payments.

PayID® means the identifier you choose to use to receive NPP Payments.

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

PayID Service means the central payment addressing service which is available for addressing NPP Payments.

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

Payment means a payment transacted using the Facility, including access to the BPAY facility and transfers to external parties.

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

Periodical payments means recurring payments that are made daily, weekly, fortnightly, monthly, annually or at other regular intervals, but does not include direct debit arrangements or direct credit arrangements.

Receiving ADI means an ADI whose customer has received an internet payment.

Regular Payment means direct debit arrangements, direct credit arrangements and periodical payments.

Sending ADI – means an ADI whose customer has made an internet payment.

Unintended recipient means the recipient of funds as a result of a Mistaken Internet Payment.

User means an account holder or an individual authorised by an account holder to perform transactions using a facility held by the account holder.

Visa card means the Visa debit issued to you or an additional cards by Fire Service Credit Union.

We, us, our and Credit Union are references to Fire Service Credit Union Limited ABN 17 087 651 152.

You, your or yours are references to you, the account holder(s) in respect of the account from which you instruct us to process a transaction.

1. Reporting Lost/Stolen cards

In person: 22 Chancery Lane Adelaide during office hours

Phone: (08) 8227 2222 during office hours

Digital Banking: under Card Controls

Card Hotline for Visa cards available 24/7

After hours: 1800 648 027

Overseas: +61 2 8299 9101

2. Changes to these terms and conditions

We may change these Terms and Conditions, change the fees that apply, or impose new fees with sufficient notification. We may change fees, charges, interest rates and other conditions at any time.

The following table sets out when we will notify you of any change.

Type of Variation	Minimum Notice
Introducing or Increasing of any fee/charge*	30 days
Changes to fee free transactions	20 days
Change in interest rates	Day of the change
Changing the method by which Interest calculated	20 days
Changing the frequency with which interest is debited or credited	20 days
Balance ranges to which interest rates apply	20 days
Imposing, removing or adjusting daily or periodic transaction limit	20 days
Increasing your liability for losses EFT transactions	20 days
Minimum balance to which an account fee applies	20 days

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

For all other changes not included in the above table, we will provide reasonable notice (which, depending on the nature of the change, may be before or after the change is made). If we reasonably consider that such a change is unfavourable to you, we will provide at least 30 days' notice. However, we may give shorter, or no, advance notice of a change unfavourable to you if it is reasonable for us to manage a material and immediate risk.

3. Notices and Electronic Communications

We may notify you of changes to your account and access facility in any way allowed by law and, where it applies, the ePayments Code. This may include one or more of the following:

- On or with your next statement
- Post, to your last known residential or postal address
- Via our website or newsletter
- Through Internet Banking or Mobile Banking App
- By email
- Media advertisements

We will always give you notice in accordance with any applicable laws or industry codes (such as the Customer Owned Banking Code of Practice), or any other terms and conditions applicable to your account, which require minimum notice periods or specific methods of notification.

When deciding how to notify a change, we will consider the nature and extent of the account change, as well as the cost and effectiveness of different methods of notification. We will use your contact information on our records. You must notify us whenever you change your contact details.

To the extent permitted by law, we may provide you any notice or other information in writing, electronically or by telephone, or by telling you that the information is available on our website of other electronic forum.

Electronic means may include:

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

You may elect to receive notices and other communications and documents we are required to give you in writing by post at any time by changing your communication preference by contacting us. If you make this election, you will also be taken to have elected to receive statements of account for all your deposit accounts and credit contracts by post.

General Information

4. Customer Owned Banking Code of Practice

The Customer Owned Banking Code of Practice (Code) is the code of practice for Australia's mutual banks, credit unions and building societies.

The Code is an important public expression of the value we place on improving the financial wellbeing of our individual members and their communities.

Our promises to you

We will comply with the Code in our dealings with you.

Our Code obligations include the following key promises that we make to you as our customers and owners:

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

You can request a copy or download a copy of the Customer Owned Banking Code of Practice from our website https://www.fscu.com.au

5. The Customer Owned Banking Code Compliance Committee

The Code is administered by the Code Compliance Committee (the COBCCC), an independent committee established to monitors and oversee compliance with the Code. Their purpose is to ensure that we as subscribers of the Code meet consistent and high-quality service standards are maintained for the benefit of customers. They do this by monitoring Code compliance, engaging with stakeholders and analysing the financial services environment.

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

- Phone: 1800 931 678
- Email: info@codecompliance.org.au
- Post: PO Box 14240 Melbourne VIC 8001

6. Complaints and Dispute Resolution

If you have a complaint about our products, services, staff or the handling of a complaint, please let us know. We will investigate the matter and attempt to address your complaint as soon as practicable.

Please refer to our Dispute Resolution Guide which forms part of these Terms and Conditions. This guide outlines the dispute process and is available on our website or from our office.

There are several ways you can contact us:

- In Person: 22 Chancery Lane, Adelaide
- Phone: 08 8227 2222
- Email: fscuhelpdesk@fscu.com.au
- Post: 22 Chancery Lane, Adelaide SA 5000

Our external dispute resolution scheme for independent arbitration is the Australian Financial Complaints Authority (AFCA). You can contact AFCA as follows:

- Phone: 1300 931 678 (free call)
- Email: info@afca.org.au
- Website: www.afca.org.au
- Post: GPO Box 3, Melbourne Vic 3001

7. ePayments Code

The ePayments Code regulates electronic payments including ATM, EFTPOS card transactions, online payments, Internet and Mobile Banking and BPAY

We warrant that we will comply with the ePayments code.

8. Financial Claims Scheme (FCS)

The Financial Claims Scheme (FCS) is an Australian Government scheme that provides financial protection for depositors of authorised deposit taking institutions (ADIs). Deposit accounts with funds in Australian dollars up to a limit of $250,000 for each account holder at each bank, building society, or credit union incorporated in Australia and licensed by APRA. In the unlikely event of an ADIs insolvency, account holders will be allowed quick access to deposits that are protected under the FCS. More information is available at www.fcs.gov.au.

9. Privacy

Your privacy is important to us. Fire Service Credit Union is bound by the Australian Privacy Principles under the Privacy Act 1988 (Cth) and has its own Privacy Policy. If you do not provide us with personal information we request, or provide us with incomplete or inaccurate personal information, it may not be possible to provide you with an account, an access facility, process your transactions, or resolve a complaint or disputed transaction if one arises.

You consent to us disclosing your personal information to third parties where doing so is necessary for us to process your instructions in relation to an account or access facility (eg to Cuscal Ltd or BPAY Pty Ltd in order to process a transfer or payment).

We also collect personal information about any signatories you nominate.

You may have access to the personal information we hold about you at any time by asking us. For further information on our obligations regarding your personal information, how we collect, hold, use, and disclose this information refer to our Privacy Policy either at our website or from our office.

Our Privacy Officer's contact details are:

- Phone: 08 8227 2222
- Email: fscuhelpdesk@fscu.com.au
- Post: 22 Chancery Lane, Adelaide SA 5000

10. Fees and Charges
Our 'Fees and Charges' brochure forms part of these Terms and Conditions and sets out the fees and charges that are currently payable in relation to our products and services.

11. Financial Hardship Assistance
Occasionally some members face financial difficulty. We encourage you to tell us at an early stage if you are experiencing financial difficulty. We understand life can take unexpected turns but, whatever the circumstances, we are committed to assisting and supporting any members who face financial difficulty. If you are experiencing financial hardship or difficulty, please contact us.

12. Accessibility
If you are deaf, have a hearing impairment and/or have a speech impairment we welcome calls through the National Relay Service (NRS). Visit the NRS website to choose your preferred access point, or call the NRS Helpdesk on 1800 555 660 for assistance.

If English isn't your first language, you can access a free interpreter service through Translating and Interpreter Services (TIS). This service is provided by the Department of Home Affairs and is available in over 150 languages. You can ask our staff to arrange this service for you at our branch or over the phone. Account Terms and Conditions.

13. Use of our account and access facilities
You and an authorised user may not use our access facilities to engage in conduct that, in our opinion is offensive or inappropriate or if we suspect any type of abuse. We may block, restrict access or close your account in order to protect another person.

This may include:

- If you have misused your account to engage in financial abuse or any other types of abuse which may involve taking away access to money, manipulating financial decisions or using money without a person's consent
- Where you have been found to use offensive language in payment descriptions, including but not limited to, swear words or profanity, discriminatory remarks, or the threat of abuse.

Your Account

14. Membership
You need to become a member of FSCU before you can open any accounts and use our Access facilities. We offer membership to Emergency Services Employees and their families and other approved persons as defined in the Constitution of the Credit Union. If you are not an Emergency Services Employee we may ask for evidence of eligibility such as a letter of introduction from an eligible member. You will need to subscribe to a $10 share which is to be paid at the time of applying for membership.

Memberships may be opened for non-personal use (e.g. clubs, societies) but must be opened in the name of a separate legal entity.

We may decline an application for membership in accordance with our Constitution, acting reasonably. On becoming a member you agree to be bound by the Constitution of FSCU and any registered amendments.

15. Proof of identity required
We are required by law to verify your identity before opening or allowing access to an account and any person you appoint as a signatory on your account. We may need to obtain additional information from you such as the source of funds in your account or how you plan to use your account.

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

- current Australian driver's licence
- current Australian passport (or one that has expired within the last 2 years)

- a proof of age card which contains a photograph issued by an Australian State or Territory.

If you do not have photo ID, please contact us to discuss what other forms of identification may be acceptable. If you are unable to attend our Office you will need to be identified by the Document Certifier process as detailed on the Certification Form.

For a child under 18 years of age, different Identification requirements apply. A Birth Certificate, Notice issued by a School Principal within the last three months, or Student Identification card are also suitable identification documents.

16. Tax Identification Number

You may wish to quote your Tax File Number (TFN) or Exemption to us, however this is not compulsory. If you do not quote your TFN or Exemption we are obligated to deduct Withholding Tax from interest earned at the top marginal rate.

For Joint accounts, Withholding Tax will be deducted unless each account holder has quoted their TFN or Exemption.

Your TFN or Exemption will be applied to all accounts under your Membership. We will also apply your TFN or Exemption to any accounts you subsequently open unless you advise us otherwise.

For Non-Personal accounts you may quote your Australian business Number (ABN) instead of your TFN.

If you have a tax liability in a country other than Australia, you must provide us with your Taxpayer Identification Number and Country.

17. Transactional Accounts

17.1 Everyday Account (S1)

The Everyday savings account is designed as a daily transactional account with easy access to your money. Includes no longer available accounts designated as S2, S3, S4, S6.

17.2 Home Loan Offset Accounts (S9)

The Offset account is a deposit or savings account which is designed to help reduce the interest which accrues on a home loan. To be eligible for an Offset account you must have an eligible home loan to link the Offset account to. If you have an eligible home loan you can request an offset account.

Offset accounts can only be linked to selected FSCU home loans. You can find out which home loans are eligible for an Offset facility (“eligible loans”) by contacting us. You may link up to four offset accounts to an eligible home loan subject to these terms and conditions.

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

If the balance of your linked transaction account is zero or in debit; or the balance of your home loan account is zero or in credit, the mortgage offset facility is not applied.

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

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

Your home loan offset facility will be cancelled if:

- you request us to cancel the facility; or
- the facility is no longer offered by us; or
- either your home loan account or your home loan offset account is closed.

Using the home loan offset facility does not affect any of your obligations under your Offer and Loan contract or any other provisions of the Consumer lending terms and conditions. You must continue to meet all your obligations including, without limitation, any agreed repayment amount.

17.3 Insurance/Budget Account (S10)
The insurance/Budget account is predominantly designed for health insurance payments. It may be used for other direct debits for paying and saving for regular bills. It allows you to separate your money from other accounts to help you budget for your expenses.

17.4 Retiree Access Account (S20)
The Retiree Access account is designed as an account for the retired member and can be used as a daily transactional account. The Retiree Access Account is available for Natural Persons only in receipt of a retirement income

17.5 Business Account (S21)
The Business Account is an account designed for your small business. Business accounts are only available to members who hold one membership share in FSCU.

18. Savings Accounts

18.1 High Return Savings Account (S5)
The High Return savings account is designed for the saver who wishes to attract higher interest on their savings. Unlimited deposits, including Direct Credits may be made to the account however withdrawals are limited to one (1) free withdrawal per calendar month. Any additional withdrawal will attract a fee. Please refer to the fees and charges brochure.

18.2 Christmas Savings Account (S7)
The Christmas savings account is designed for savings during the year to provide funds for the Christmas period. Funds deposited to the Christmas savings account will be available for withdrawals, including through Internet Banking, from 1 November to 31 January each year. There is no withdrawal access outside this time.

18.3 Investment Savings Account (S8)

The Investment Savings Account is designed to separate savings and spending.

18.4 Junior Firefighter Account (S12)

The Junior Firefighter savings account has been designed for members under the age of 18 to save funds.

19. Opening a Child's Accounts

Accounts may be opened by a parent, relative or legal guardian on behalf of a child (defined as under 18 years).

A membership will be opened in the name of the child. The child will be a member. To open the membership, the child's identification must be provided. The child will be the owner of the membership and the account. The child will also hold the taxation liability for any interest earned.

A child qualifies for a Junior Firefighter savings account which is an account specifically designed as a children's savings account. Other savings and fixed term deposit accounts may also be opened for the child.

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

- you acknowledge that any credit balance held in the account is the property of the child;
- you may be an authorised signatory on the account or appoint another authorised signatory;
- the child can access the account at the earlier of us receiving your written consent or the child attains the age of 18;
- you may authorise the child to have access to the account at any time after the child attains the age of 12 and can register a consistent signature (in exceptional circumstances we may consider such a request for children under the age of 12); and

- upon attaining the age of 18, the child will have automatic access to the account by presenting sufficient identification and registering a signature with us.

When an account is opened for a child, there is no access to any funds in the child's account until the child registers a signature, exceptions may be made for withdrawals that are for the benefit of the child (e.g. a cheque withdrawal in the child's name for further investment).

The parent, relative or legal guardian as an authorised signatory can have view only access on Internet Banking. This gives access to account information but not for withdrawals until the child has registered a signature.

A child over 12 years may open and operate a membership and account in their own name without the permission of a parent or legal guardian.

When the child turns 18 years, they are now an adult and therefore are no longer be eligible for a Junior Firefighter savings account so the account will be closed and funds will be transferred into a new account on their membership. Any other accounts held, Internet Banking & Visa debit cards are unaffected.

CARD ACCESS: Visa Debit Card access linked to a child account is generally for a child aged 12 years plus. Approval outside of these circumstances will be at the discretion of the Chief Executive Officer. Visa Debit cards are linked to a separate S1 Everyday Account not a S12 Junior Firefighter Savings Account.

20. Fixed Term Deposits

Fixed Term Deposit accounts are made on the basis of your agreement to deposit your funds with us for a fixed period of time at a guaranteed rate of interest. The interest rate will not change during the fixed term.

We reserve the right to set minimum and maximum amounts for deposits and terms. Please refer to the Interest Rate Schedule available on our website or from our Office for the minimum and maximum deposits and terms available.

Deposits over the maximum amount on the schedule are subject to acceptance and negotiation. We may refuse to accept any deposit.

20.1 Interest

Interest is calculated daily and can be paid monthly, quarterly or on maturity, interest may be:

- paid into another account you have with us; or
- if your interest is payable at maturity, reinvested with the original Term Deposit amount for another term of your choice.

20.2 When your Term Deposit matures

On the Term Deposit maturity date, the principal and any interest which has accrued but not been paid, will become payable to you. We will notify you that your Fixed Term Deposit is maturing approximately two (2) weeks prior to the maturity date.

Prior to the maturity date you may notify your intention at maturity of either:

- withdrawing the Term Deposit (and any interest accrued but not paid); or
- reinvesting all or part of the Term Deposit (and any interest accrued but not paid) for a further term of your choice.

If you notify us of your intention to withdraw, the Term Deposit funds will be transferred to another account with us on the date of maturity. If you notify us to reinvest all or part of the Term Deposit for a further term, we will reinvest it in accordance with your instructions. If you do not notify us of your intention to withdraw or reinvest prior to maturity, the Term Deposit (and any interest accrued but not paid) will be automatically reinvested for a further term of the same duration or the nearest available duration if a Term Deposit for the same duration is no longer available. A lower interest rate may apply after reinvestment.

If you do not advise your instructions prior to maturity and we reinvest your Term Deposit for a further term, you will have a grace period of 7 calendar days, starting from the maturity date, to advise us of any alternative instructions you would like to make regarding your Term Deposit, without incurring a fee.

Changes you make during the grace period, such as changing the term or withdrawing funds, may result in a different applicable interest rate.

20.3 Adding to Your Term Deposit

You may only add to an existing Term Deposit upon maturity. If you wish to deposit additional funds to an existing Term Deposit, you may do so by notifying us prior to maturity or within the 7 day grace period immediately following maturity. These additional funds will only be added to the Term Deposit from the maturity date. If you want to deposit additional funds for a fixed period, prior to your existing Term Deposit maturing, you will need to open a new and entirely separate Term Deposit.

20.4 Withdrawing Funds from you Term Deposit

The Fixed Term Deposit is made on the basis that it is not withdrawn before the date of maturity. However, if you wish to withdraw the whole or part of a Term Deposit prior to maturity, you must provide us with not less than 7 days written notice. An administration fee and interest penalties apply to an early withdrawal, backdated to the date of the deposit. If we have already paid interest on the deposit subject to early withdrawal (for example if interest had been paid monthly) we may deduct the penalty interest from the balance of the funds withdrawn. Refer to the Fees & Charges brochure for details on fees and charges.

No fee or reduction in return will be applied if the withdrawal is as a result of the death of an owner of the Term Deposit.

The balance which remains in a Term Deposit following a partial withdrawal will continue to earn the contracted rate of interest until maturity if the contracted rate would have applied to this amount when it was initially deposited. If the remaining balance would have earned a lower rate of interest when it was originally deposited, that lower rate will apply to the remaining balance as from the date of the partial withdrawal.

21. Joint Accounts

A joint account is an account held in the name of more than one natural person. The important legal consequences of holding a joint account are:

- The right of survivorship – when one joint holder dies, the surviving joint holder(s), automatically take the deceased joint holder's interest in the account.
- Joint and several liability – each joint holder is individually liable for the full amount owing on the joint account and any transactions conducted on that joint account.

The account can be operated on an "either to sign" or "all to sign" basis:

- 'Either to sign' means any one joint account holder can authorise any action on the account including closure of the account and internet banking transactions.
- 'All to sign' means all joint account holders must sign must authorise any action on the account, including closure of the account.

All joint account holders must consent to the joint account being opened on an 'either to sign' basis. However, any one joint account holder can cancel this arrangement, making it 'all to sign' or can request an account to be suspended to allow the joint account holders time to reach agreement about dispersal of the account funds and we will comply with such a request.

This paragraph does not, for example, apply to an account in a single name but with multiple signatories – e.g. a company account where directors are co-signatories on behalf of the company.

22. Trust and Self-Managed Superannuation Funds

Existing members may open savings accounts and Fixed Term Deposits for their Trust or Self-Managed Superannuation Funds (SMSF). However:

- we are not taken to be aware of the terms of the Trust; and
- we do not have to verify that transactions you carry out are authorised by the Trust or permitted by legislation.

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

23. Authority to Operate (Signatories)

You may authorise a person(s) to operate on your accounts. This must be in writing and we require the authorised person to be identified by us prior to accessing any account. Such an authority will apply to all accounts under your membership unless you specify otherwise and you will be liable for any debts incurred by them when using your account.

You should ensure that the person you authorise to operate on your account is a person you trust fully.

You may revoke the authorised person's authority at any time by written notice to us. The authority to operate will also cease to have effect upon the death of the member granting the authority.

By granting authority to operate your accounts, you allow the person/s to:

- carry out deposits, withdrawals and transfers on the nominated account(s)
- enquire about balances and transactions on any nominated account(s)

We are not liable for any loss or damage caused to you by persons you have authorised to operate on your accounts except for loss or damage arising from fraud or other misconduct by us or our employees or if we are liable under a statute or the ePayments Code including, but not limited to, when you have instructed us to cancel their access and the loss or damage occurred after your instructions are given to us.

You may revoke the authorised person's authority at any time by written notice to us. The authority to operate will also cease to have effect upon the death of the member granting the authority.

24. Interest Calculations

Our Deposit Accounts Interest Rates and Summary of Accounts document, available from our website or our Office, forms part of these Terms and Conditions. The document provides information about our savings account and Fixed Term Deposit interest rates including when interest is paid. We may vary the interest rates from time to time. Fixed Term Deposit interest rates remain fixed for the agreed term.

Interest is calculated on a daily basis on your closing account balance. The daily interest rate is the relevant account interest rate divided by 365 (or 366 in a leap year). The interest is accrued until credited to your savings account, or in the case of Fixed Term Deposits, as per your instructions. Interest earned is income and may be subject to income tax.

From time to time we may offer a higher rate or bonus rate to certain account holders or funds subject to a specified criteria and specific time period. Details of any offer including eligibility, how interest is calculated, how interest is paid, and any withdrawal restrictions will be publicised in promotional material available on our website and from our office during the relevant period.

24.1 Tiered interest rates

If an account has tiered interest rates, different interest rates apply to different parts of your account balance. You receive a certain rate of interest on that part of your account balance that falls into a particular band of amounts. For example, the interest paid on the part of your account balance between $10,000 and $20,000 may be different to the interest paid on the balance up to $9,999. From time to time, some tiers may have the same interest rate. You should note that we may vary account terms to change the tiers. If an account has a tiered interest rate, interest is calculated by multiplying that part of the account balance that falls into a particular band by the daily interest rate applying to that band, and then adding together the interest payable in each band.

25. Account Combination

We may set off the credit balance of any of your deposit accounts and the value of your membership share against any debt owing by you to us.

This may become necessary if, for example one of your accounts becomes overdrawn or in payment of any amount overdue on any loan account in the same name or business account operated by you.

Only credit funds held in an account in the same name may be utilised for this purpose. We will not use funds held in your name that you have told us are held on trust for a Child for this purpose. We may do this so long as where combining accounts would not breach the Code of Operation for Centrelink Direct Credit Payments. We will give you written notice promptly after exercising any of these rights.

26. Overdrawn Accounts

You are responsible for maintaining sufficient cleared funds in your account to cover all direct debits and electronic transactions. If you do not, we may do any of the following:

- dishonor the transaction;
- 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 withdraw more than the available balance from your account, the amount overdrawn is immediately payable by you without further demand by us.

Your available balance is comprised of cash deposits, direct credits processed to your account and any available credit we have provided such as an Overdraft. Any outstanding card transactions are subtracted from the available balance.

You may be charged an overdrawn account fee and be liable for any reasonable legal fees we incur in recovering the overdrawn amount from you. The Default Rate of Interest is payable on Overdrafts over the approved limit and Overdrawn Savings accounts with no pre-approved limit. See our Deposit Account Interest Rates and Summary of Accounts and Fees & charges Brochures on our website.

27. Closing a Membership

You may resign your membership at any time by completing a Resignation Request form or by notifying us in writing subject to the following conditions:

- If your account(s) are in debit you must pay the outstanding balance, plus any outstanding accrued interest, fees and charges and pending transactions
- You have returned the cards used to access your accounts

Refer to closing an account.

28. Closing an Account and Access Facilities

You can close accounts and an access facility at any time. To close an account your instruction must be in accordance with the account operating authority if more than two signatures are required.

You will be required to return or provide evidence that you have destroyed any Access Cards. We may defer closure and withhold sufficient funds to cover payment of outstanding fees and electronic transactions.

Acting reasonably, we may close your account and Access facilities due to unsatisfactory conduct or any other reason we consider appropriate such as to protect us and/or you from a legitimate risk. We will provide 14 days' notice to your last known address and pay you any credit balance.

We may without prior notice close, suspend your access to any account, cancel any access facility, or delay, block, freeze or refuse any transaction if we reasonably believe doing so will protect you or us from harm or loss.

29. Deceased Accounts

In the case of joint accounts, the law of survivorship and liability applies.

For single accounts, once we are notified of the member's death any account in their name will be restricted pending instructions from the Executor(s) or Administrator(s). Any Authority to operate ceases to have effect.

We have the ability to appropriate any credit balance held in the deceased's account towards the repayment of any debt owed to us.

Until finalisation of the Estate, funds can only be drawn for funeral expenses and any Estate costs by providing us with a tax invoice (or equivalent) acceptable to us.

30. Account Statements

We will provide you with regular account statements at least every 6 months clearly setting out all transactions relating to your accounts with us. We will send these account statements to the last address you have given us, unless we reasonably believe that this is no longer your correct address.

You can ask us for more frequent account statements at any time, we may charge a fee for providing more frequent statements however we may waive this if we are satisfied that your circumstances warrant this.

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

We will provide your statement electronically if you have Internet Banking.

For joint accounts we will only send one Statement to the primary joint member. Joint account holders may request to receive statements at any time.

We recommend that you check your account statement as soon as you receive it. Immediately contact us using one of the contact methods on the back of this document if you would like to query any entries on your statement.

If you do not wish to receive account statements and other information provided with account statements electronically, you may elect to receive paper account statements by post by contacting us or using Internet Banking. We may charge a reasonable fee, reflecting our costs (although we may waive this if we are satisfied that your circumstances warrant this).

If you decide to receive paper account statements by post you will no longer be able to view your previous eStatements using Internet Banking. You should print or save a copy of your eStatements before requesting to receive paper account statements by post.

31. Dormant Accounts and Unclaimed Monies

Your membership and/or account will become dormant if you have not made any deposits or withdrawals for 12 months s (other than transactions initiated by us, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep the account open. If you do not reply we will treat your account as dormant

If this occurs, we may:

- charge a dormant account fee
- stop paying interest or reduce the amount of interest

If the balance of the dormant account is less than the fee, the account may be closed and the proceeds retained as the fee. If you do not have any other active accounts, your membership may be terminated. If the balance in the dormant account is less than $500, the account may be closed. If the balance in the dormant account is more than $500, and you have not made any deposits or withdrawals during a continuous 7 year period, the account may be closed and the proceeds transferred to the Australian Securities and Investments Commission unclaimed money fund.

32. Change of personal details

If you change your personal information (e.g. change your name, address or contact details) or choose to revoke the authority of any signatory, appoint a new signatory or add a temporary restriction, you must contact us and advise us of the change.

Alternatively, you can make certain changes to your Account yourself within the Mobile Banking App or Internet Banking, including changing your address and contact details

You must notify us promptly of any change to your name or address for the mailing of any notifications and statements which we are required to send to you.

33. Accounts and access facilities

The following table provides a summary of key features and access facilities that may be permitted on 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

Deposit Account Type	S1 Everyday	S9 Home Loan Offset	S10 Insurance /Budget	S20 Retiree Access	S21 Business	S5 High Interest	S7 Christmas Club	S8 Investment	S12 Junior Firefighter
Eligibility	**All members**	**Eligible home loans**	**All members**	**Retired members**	**All members**	**All members**	**All members**	**All members**	**Member <18 years of age**
Funds available at call	✓	✓	✓	✓	✓	✓	✓[2]	✓	✓[1]
Visa Card access	✓	✓	×	✓	✓	×	×	×	×
Optional Overdraft	✓	×	×	✓	✓	×	×	×	×
Monthly access fee	×	×	×	×	×	×	×	×	×
Transaction Withdrawal fee	×	×	×	×	✓[3]	✓[4]	×	×	×
Internet and Mobile Banking	✓	✓	View only	✓	✓	✓	✓[2]	✓	✓[1]
BPAY®	✓	✓	✓ Staff Assisted	✓	✓	×	×	✓	×
EFTPOS purchase and cash out	✓	✓	×	✓	✓	×	×	×	×
ATM withdrawal	✓	✓	×	✓	✓	×	×	×	×
Direct Credits	✓	✓	✓	✓	✓	✓	✓	✓	✓
Direct Debits	✓	✓	✓	✓	✓	×	×	✓	×
NPP Payments	✓	✓	×	✓	✓	✓	✓[2]	✓	✓[1]
Periodical payments	✓	✓	✓	✓	✓	×	×	✓	×
Branch Transaction	✓	✓	✓	✓	✓	✓	✓[2]	✓	✓[1]
Corporate cheques	✓	✓	✓	✓	✓	✓	✓[2]	✓	✓[1]

Round up origin account	✓	✓	×	✓	×	×	×	×	×
Round up destination account	✓	✓	×	✓	×	×	×	✓	×

[1]Access is permitted where the child has registered a signature and is over 12 years of age
[2]Only between November 1 and January 31 annually
[3]Refer to the Fees and charges brochure for full details
[4] free withdrawal per month then $5.00 for each subsequent withdrawal in the month

Accessing your Account

34. Deposits to your Account

You can make deposits to your account in the following ways:

- Cash at our Office
- Direct Credits and Payroll
- Transfer from another FSCU account
- Electronic Transfer from another Financial Institution

You should note that electronic deposits may not be credited on the same day.

35. Withdrawals or Transferring from your Account

You can make withdrawals and transfers from your accounts in the following ways:

- Cash withdrawals at our Office
- Credit Union Corporate Cheque
- Direct Debit
- Internet Banking including Mobile Banking
- BPAY
- ATM and EFTPOS with a Visa Debit card

Please refer to the Fees and Charges brochure for details on fees that may apply to these Access methods.

Cash may be obtained through ATMs and some EFTPOS terminals (EFTPOS terminals solely at Merchant's discretion) up to the combined ATM and EFTPOS daily transaction limit of $1000. On request your Card limit may be temporarily increased.

If you wish to perform a cash withdrawal, at our Office, in excess of $1000 a minimum of 24 hours notice will be required.

36. Transaction Limits

We limit the number of transactions that can be made on any one day according to the type of Access method. Acting reasonably, we may reduce transaction limits to zero for security reasons at any time. You should note that individual Merchants, BPAY Billers and other Financial Institutions may impose their own EFT transaction limits. The following withdrawal limits apply:

Transaction type	Limit per day
Cash withdrawals over the counter at the branch with prior arrangements	$1,000
Cash withdrawal using a card at ATMs, EFTPOS and Visa purchases with cash out	$1,000

Visa card when you select credit account of make purchases of goods or services online	Up to your available balance
PayWave contactless transactions via Visa card or digital wallet	$100 per transaction up to maximum 15 transactions or $500 per card per day.
BPAY transaction	$10,000
Transfer to another financial institution via internet or mobile banking	$2,000
Internal transfer to another FSCU account via internet or mobile banking	$20,000
Overseas telegraphic transfer via internet or mobile banking	$500

On request your card and Internet Banking transfer limits may be temporarily increased.

37. Direct Credits

You may arrange direct credits into your account. You will need to provide our BSB (805-013), your account number and your Surname to the person or organisation that will be depositing funds to your account. 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 delay in crediting your payment to 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.

38. Credit Union Corporate Cheques

This is a cheque made payable to the Payee you nominate. You can purchase Credit Union Corporate Cheques from our Office. A fee applies. Please refer to our Fees and Charges brochure.

You should note that we cannot stop payment on a Credit Union Corporate Cheque if you used it to buy goods and services and you are not happy with them. In this instance you must seek redress from the provider of the goods or services.

If a corporate cheque is lost or stolen, you must immediately report the incident to us so that we can place a stop on the cheque. You will also be required to indemnify us from claims that you wrongfully authorised stopping the cheque.

39. Direct Debits

A direct debit facility is a simple and convenient way for you to make payments straight out of your transaction account. It is most often used for regular transactions like insurance premiums and utility bills. To pay by direct debit, you sign a Direct Debit Request (DDR) form addressed to the business or company (the biller) that you wish to pay. The DDR gives the biller permission to debit amounts from your transaction account. You will need to provide the biller with our BSB number (805-013) and your account number. The account information you provide to the biller 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 being provided by you.

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

You should note that this does not apply to recurring payments. A recurring payment is a regular automatic payment set up from your debit card with a merchant or service provider. To do this, you will need to

arrange a direct debit authority and supply the merchant or service provider with your card number, expiry date and three digit CVV number on the back of your card. This allows the merchant or service provider to charge your debit card. These are covered under Visa Scheme rules.

39.1 How to stop Direct Debits

To cancel the DDR you can contact us, we will stop the facility within 1 business day. We suggest you also contact the biller without delay to avoid any fees the biller may charge for a rejected direct debit. If you have multiple Direct Debits from the same biller, you must also contact the biller to ensure the correct debit is stopped and that your other debits are still paid as all debits from the one biller could be stopped. We will not charge you a fee for cancelling a direct debit facility.

We will accept and process your complaint that a direct debit was not authorised or is otherwise irregular. However, you may also contact the biller to resolve the complaint.

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

We have the discretion to (but under no obligation to do so) pay a Direct Debit and overdraw your account for this purpose. We will also charge a Direct Debit honour fee as detailed in the Fees and Charges brochure.

40. Periodical Payments

Periodic Payments allow us to debit your account with a pre-arranged amount and send it to another account or to a third party. You can arrange this by contacting us or you can log on to Internet/Mobile Banking and establish a regular payment arrangement.

The Periodical Payment authority will remain in force until either:

- The cancellation date you have nominated, or
- You request us to cancel or amend the authority, or
- Authority is cancelled by you via Internet/Mobile Banking, or
- Notice of death or bankruptcy of a member is received.

Periodical Payments can be paid electronically to external parties or transfers to other FSCU accounts. If the due date is a weekend or public holiday payment will be made on the next business day.

We will only make a Periodical Payment if there are sufficient clear funds in the account on the nominated date for transfer. At our discretion we may search for clear funds for up to 5 days. You may be charged a fee if payment cannot be made. If sufficient clear funds are not in your account on more than 5 consecutive occasions (after 5 attempts on each occasion) we will cancel the Periodical Payment authority. We will advise you in writing.

If the Periodical Payment is for a loan with us and there are not sufficient funds to make the payment, we may at any time debit your account from which the payment is made for any amount up to the amount due. However, we will not overdraw your account or exceed any credit limit in doing so.

Electronic Banking Access Facilities and ePayments Conditions of Use

41. Information about our ePayment facilities

You should follow the guidelines below to protect against unauthorised use of the mobile banking app, internet banking or your access card and passcodes.

These ePayment Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:

- initiated using electronic equipment, and
- not intended to be authenticated by comparing a manual signature with a specimen signature.

These ePayment Conditions of Use apply to the following transactions:

- electronic card transactions, including ATM, eftpos, credit card and debit card transactions performed by digital or physical card that are not intended to be authenticated by comparing a manual signature with a specimen signature
- telephone banking and bill payment transactions,
- pay anyone banking facility transactions
- online transactions performed using a card number and expiry date
- online bill payments (including BPAY)
- direct debits
- transactions using mobile devices

42. Security of Access Devices and Passcodes

These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised payments. Liability for such transactions will be determined in accordance with these ePayments Conditions of Use and the ePayments Code. If you fail to ensure the security of your access card, access facility and passcodes you may increase your liability for unauthorised transactions.

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

- Visa Card
- BPAY®
- Internet banking
- Mobile banking

You can use any of these electronic access facilities to access an account, as listed in the Summary of accounts and of access facilities.

You should follow the guidelines below to protect against unauthorised use of your access card and passcode.

What you need to know before you use a device to make Electronic Payments:

- Sign your card as soon as you receive it.
- Keep your card in a safe secure place and check regularly to ensure that your card is not lost or stolen
- Carry your access card whenever possible
- Where your device can be accessed by a biometric identifier such as fingerprint login, ensure only your biometric identifier is registered on that 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.

- Familiarise yourself with your obligations to keep your access card and passcodes secure.
- Familiarise yourself with the steps you have to take to report loss or theft of your access card or to report unauthorised use of your access card, BPAY® or internet banking.
- If you change a passcode, do not select a passcode which represents your birth date or a recognisable part of your name.
- Never write the passcode on the access card.
- Never write the passcode or PIN on anything which is kept with or near the access card.
- Never lend your card or device to anyone or permit another person to use your card or device.
- Remove any card from your device before you dispose of your device.
- Never tell or show the passcode to another person.
- Use care to prevent anyone seeing the passcode being entered on a device.
- Keep a record of the Visa card number and the Visa Card Hotline telephone number for your area with your usual list of emergency telephone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address.
- Always access the internet banking service only using the official URL addresses (www.fscu.com.au.)
- If accessing internet banking on someone else's PC, laptop, tablet or mobile phone, always delete your browsing history.
- Always reject any request to provide or to confirm details of your passcode. We will NEVER ask you to provide us with these details.

43. Biometric identifier

If you enable a biometric identifier such as fingerprint or face identifier login in the mobile banking app settings, we may permit you to login into mobile banking app using the registered biometric identifier on that device. You can still login to the mobile banking app using the passcode that is registered to your account. When you log into the mobile banking app using your biometric identifier, you instruct us to perform any transactions requested during the mobile banking app session.

Warning: If you enable the biometric identifier login option, then any of the biometric identifiers stored on your device can be used to log into the mobile banking app. You must ensure that only your biometric identifier (and not any other person's) is stored on the mobile device to access the mobile banking app. We strongly recommend that at all times you should use your passcode to access the mobile banking app.

44. When you are not liable for loss

44.1 You are not liable for losses caused by unauthorised transactions if the cause of the loss is any of the following:

a. fraud or negligence by our employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent,
b. a device, identifier or passcode that is forged, faulty, expired or cancelled,
c. a transaction requiring the use of a device and/or passcode that occurred before a user received the device and/or passcode (including a reissued device and/or passcode),
d. a transaction being incorrectly debited more than once to the same facility, and
e. an unauthorised transaction performed after we have been informed that a device has been misused, lost or stolen, or the security of a passcode has been breached.

44.2 You are not liable for loss arising from an unauthorised transaction that can be made using an identifier without a passcode or device. Where a transaction can be made using a device, or a device and an identifier, but does not require a passcode, you are only liable only if the user unreasonably delays reporting the loss or theft of the device.

44.3 You are not liable for loss arising from an unauthorised transaction where it is clear that a user has not contributed to the loss.

44.4 In a dispute about whether a user received a device or passcode:

a. there is a presumption that the user did not receive it, unless we can prove that the user did receive it,
b. we can prove that a user received a device or passcode by obtaining an acknowledgement of receipt from the user, and
c. we may not rely on proof of delivery to a user's correct mailing or electronic address as proof that the user received the device or passcode.

45. When you are liable for loss

45.1 If clause 44 does not apply, you may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this clause 45.

45.2 Where we can prove on the balance of probability that a user contributed to a loss through fraud or breaching the passcode security requirements in clause 46:

a. You are liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of passcode security is reported to us, but
b. You are not liable for the portion of losses:
    I. incurred on any one day that exceeds any applicable daily transaction limit,
    II. incurred in any period that exceeds any applicable periodic transaction limit,
    III. that exceeds the balance on the facility, including any pre-arranged credit, or
    IV. incurred on any facility that we and you had not agreed could be accessed using the device or identifier and/or passcode used to perform the transaction

45.3 Where:

a. more than one passcode is required to perform a transaction, and
b. we prove that a user breached the passcode security requirements in clause46 for one or more of the required passcodes, but not all of the required passcodes, you are liable under clause 46.2 only if we also prove on the balance of probability that the breach of the passcode security requirements under clause 46 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

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

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

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

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

Note: You may be liable under clause 46.5 if you were the user who contributed to the loss, or if a different user contributed to the loss.

45.6 Where a passcode was required to perform an unauthorised transaction and clauses 45.2 – 45.5 do not apply, you are liable for the least of:

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

45.6 In deciding whether we have proved on the balance of probability that a user has contributed to losses under clauses 45.2 and 45.5:

a. all reasonable evidence must be considered, including all reasonable explanations for the transaction occurring,
b. the fact that a facility has been accessed with the correct device and/or passcode, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the passcode security requirements in clause 45, and
c. the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example, the number and expiry date of a device) is not relevant to a user's liability.

45.7 If a user reports an unauthorised transaction on a debit card account:

a. we will not hold you liable for losses under clause 45 for an amount greater than your liability if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, chargeback rights), and
b. this clause does not require us to exercise any rights we may have under the rules of the card scheme. However, we cannot hold you liable under this clause for a greater amount than would apply if we had exercised those rights.

46. Passcode Security Requirements

46.1 This section applies where one or more passcodes are needed to perform a transaction.

46.2 A user must not:

a. voluntarily disclose one or more passcodes to anyone, including a family member or friend;
b. where a device is also needed to perform a transaction, write or record passcode(s) on a device, or keep a record of the passcode(s) on anything:
    I. carried with a device, or
    II. liable to loss or theft simultaneously with a device, unless the user makes a reasonable attempt to protect the security of the passcode, or
c. where a device is not needed to perform a transaction, 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 passcode(s).

Note: If you or another user breaches these passcode security requirements, we may not be required to indemnify you for loss arising from that breach. See clause45.

46.3 For the purpose of clauses 46.2 b - 46.3 c, a reasonable attempt to protect the security of a passcode record includes making any reasonable attempt to disguise the passcode within the record, or prevent unauthorised access to the passcode record, including by:

a. hiding or disguising the passcode record among other records,
b. hiding or disguising the passcode record in a place where a passcode record would not be expected to be found,
c. keeping a record of the passcode record in a securely locked container, or
d. preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

46.4 A user must not act with extreme carelessness in failing to protect the security of all passcodes where extreme carelessness means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour.

Note 1: An example of extreme carelessness is storing a user name and passcode for internet banking in a diary, computer or other personal electronic device that is not password protected under the heading 'Internet banking codes'.

Note 2: For the obligations applying to the selection of a passcode by a user, see clause 46.5.

46.5 A user must not select a numeric passcode that represents their birth date, or an alphabetical passcode that is a recognisable part of their name, if we have:

a. specifically instructed the user not to do so, and
b. warned the user of the consequences of doing so

46.6 The onus is on us to prove, on the balance of probability, that it has complied with clause

46.7 Where we expressly authorise particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the passcode security requirements in clause 46.

46.8 Where we expressly or implicitly promote, endorse or authorise the use of a service for accessing a facility (for example, by hosting an access service on our electronic address), a user who discloses, records or stores a passcode that is required or recommended for the purpose of using the service does not breach the passcode security requirements in clause 46.

46.9 For the purposes of clause 46.8, we are not taken to have implicitly promoted, endorsed or authorised the user's use of a particular service merely because we have chosen to use the service or our own purposes or has not actively prevented a user from accessing a service

47. Liability for loss caused by System or Equipment Malfunction

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

47.2 Where a user should reasonably have been aware that a system or equipment provided by any party to a shared electronic network was unavailable or malfunctioning, our liability may be limited to:

a. correcting any errors, and
b. refunding any fees or charges imposed on the user.

48. Network arrangements

48.1 We must not avoid any obligation owed to you on the basis that:

a. we are a party to a shared electronic payments network; or
b. another party to the network caused the failure to meet the obligation.

48.2 We will not require you to:

a. raise a complaint or dispute about the processing of a transaction with any other party to a shared electronic payments network
b. have a complaint or dispute investigated by any other party to a shared electronic payments network.

49. Mistaken Internet Payments

49.1 When you report a mistaken internet payment, we must investigate whether a mistaken internet payment has occurred.

49.2 If we are satisfied that a mistaken internet payment has occurred:

a. We must, as soon as reasonably possible and by no later than 5 business days from the time of the user's report of a mistaken internet payment, send the receiving ADI a request for the return of the funds.
b. the receiving ADI must within 5 business days of receiving the sending ADI's request:
   (i) acknowledge the request for the return of funds, and
   (ii) advise whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

49.3 If we are not satisfied that there has been a mistaken internet payment has occurred, we will not take any further action.

49.4 We must inform you of the outcome of a reported mistaken internet payment in writing and within 30 business days on which the report is made.

49.5 You may complain to us about how the report was dealt with including that we and/or the receiving

49.6 ADI:

a. are not satisfied that a mistaken internet payment has occurred, or
b. have not complied with the processes and timeframes

49.7 When we receive a complaint we:

a. Must deal with the complaint under our internal dispute resolution procedures, and
b. must not require the user to complain to the receiving ADI.

49.8 If you are not satisfied with the outcome of a complaint you may complain to AFCA our external dispute resolution scheme

Information about the process for retrieving mistaken payment under the ePayments Code

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

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

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

- The receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request.
- If satisfied that a mistaken internet payment has occurred, the receiving ADI must:
  a. prevent the unintended recipient from withdrawing the funds for 10 further business days, and

b. notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds.

- If the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their account.
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder.
- The sending ADI must return the funds to the holder as soon as practicable.

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

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

Process where sufficient funds are not available

- where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient funds available at that time in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must exercise discretion, based on an appropriate weighing of interests of both the sending consumer and unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should:
    a. pursue the return of funds to the total value of the mistaken internet payment,
    b. pursue the return of funds representing only a partial amount of the total value of the mistaken internet payment, or
    c. not pursue any return of funds (whether partial or total)

50. Mistaken Internet Payments Credited to your Account

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

We will advise you of the results of our investigations in writing and advise you of any further actions you can take including referring the matter to our External Dispute Resolution Service.

51. Reporting Lost, Stolen or Unauthorised use of Card, Internet Banking or Mobile App Passcode

You must tell us promptly if:

- You become aware of any delays or mistakes in processing your transaction;
- You did not authorise a transaction that has been made from your account; or
- You think that you have been fraudulently induced to make a transaction.

If you think that the security of your Internet Banking or Mobile App has been compromised you must notify us immediately. If you believe an unauthorised transaction has been made you should change the passcode.

Failing to promptly notify us of the above matters may increase your liability for unauthorised payments in accordance with the ePayments Code.

If you believe your Visa Debit card or PIN has been misused, lost or stolen or your passcode has become known to someone else you must contact us immediately during business hours or the Card Hotline at any time. You must provide the following details:

- Our name
- Any other personal information you are asked to provide to assist in identifying you and the card.

The Card Hotline is available 24 hours a day 7 days a week. They will provide you with a reference number which you should retain. If the Card Hotline is not operating when you attempt notification you must report the loss, theft or misuse of your card to us as soon as possible during business hours. You will not be liable for any losses in the period that the Card Hotline is not operating providing you report to us as soon as possible.

Reporting Lost/Stolen cards	
Office hours:	(08) 8227 2222
After hours:	1800 648 027
International:	+61 2 8299 9101

You can also report your card as lost or stolen on Internet Banking or Mobile App under Card controls.

52. Internet Banking

Internet Banking provides you with access to your account to transfer amounts, make payments, and access and update information on your accounts. You must hold an account with the Credit Union or be a signatory to an account with us to register for Internet Banking.

We are authorised to act upon all instructions given through the Internet Banking Facility using your passcode unless we actually know or strongly suspect that the instruction is fraudulent.

We will advise you from time to time of the transactions which the Internet Banking Facility will enable you to perform.

When we register you for Internet Banking, we will provide you with a default passcode to access Internet Banking. Once you have logged onto you will be asked to change your passcode. We recommend that you choose a complex passcode comprising a combination of letters (both uppercase and lowercase) numbers, symbols and special characters.

Registering for Internet Banking will automatically register you for e-statements.

You may only use the Internet Banking Facility to perform transactions that the terms and conditions of an account provide.

If you are a signatory to an account which requires more than one signatory for its operation, you may view the details of the account (such as obtaining the account balance). You cannot transact on the account using Internet Banking. All transfers and external payments may be carried out by us upon completion of the prescribed form and authorised by the signatories according to the account's operations.

We cannot affect your Internet Banking instructions if you do not provide all the specified information or provide inaccurate information.

Secure SMS is an additional authentication service for external transactions via Internet Banking, utilising a secure one-time code sent to your registered mobile phone or land line.

We do not warrant that:

- you will have 24 hours a day 7 days a week access to Internet Banking,
- data transmitted by you using Internet Banking is totally secure
- account information you access by Internet Banking is always up to date.

Except as we otherwise agree from time to time to allow future dated transactions and subject to account terms and conditions, transactions utilising the Internet Banking facility will normally be processed on the same business day or the next business day. External payments made on weekends, public holidays or after 4pm on a business day will be sent on the next business day.

Acting reasonably, we may refuse to give effect to any direction you give us in respect of a payment to be made by Internet Banking or BPAY. We are not liable to you or any other person for any loss or damage which you or that person may suffer as a result of such refusal.

53. Mobile Banking

Mobile Banking is an added feature to Internet Banking, it is not a stand-alone product. You need to be registered as a current user of Internet Banking. Not all devices may be capable of accessing and using Mobile Banking and not all Internet Banking services and features maybe available from Mobile Banking. You are responsible for obtaining or using a mobile device that is compatible with our Mobile Banking Service.

The features available to you via Mobile Banking such as the way in which you can access and use actions and transactions may differ depending on your device and may change from time to time without prior notice to you.

We may suspend or disable your use of Mobile Banking without notice at any time including if we suspect unauthorised transactions have occurred or that the app is being misused.

Mobile Banking Costs

The Mobile Banking app is free however you could incur a fee from your Mobile Network provider when you download and /or use the app. The app can be accessed when travelling outside of Australia, you should check with your provider as there can be significant roaming costs. We are not liable for any additional costs you may incur for using your mobile device, they are your responsibility.

Mobile Banking Security

When logging in to your Mobile Banking the first time you will be required to enter your member number and your Internet Banking passcode. You will need to select a four digit PIN and use it with every login from that point forward. 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 us and quote your access code to restore access.

By downloading and using the app you must:

- install the latest software and security updates onto your device
- always lock your device when not in use and set a PIN to unlock your Mobile device
- take all reasonable steps to ensure no unauthorised use of your device and
- notify us as soon as possible if your device has been lost or stolen or you become aware or suspect that your device PIN or Mobile Banking App PIN has become known to another person.
- Delete the app from your registered device before you sell, dispose or gift the device

For added security do not store passwords or access codes in your device.

54. Regular Payments by Internet/Mobile Banking

You can establish regular payments by accessing Internet/Mobile Banking. Payments can be made to another account or to an external party. Payments can only be made electronically. The conditions that apply to Internet/Mobile Banking and external payments and “Future Dated BPAY and Internet payments” apply to any regular payments you establish.

You can also amend or cancel your regular payments at any time by accessing Internet/Mobile Banking.

We will continue to make the payment until the end date you entered or you cancel the payment. Payment will only be made if there are sufficient available funds in your account at the time payment is due to be made.

55. External Payments

This facility enables you to transfer funds to an account at another Financial Institution within Australia by accessing Internet Banking/Mobile Banking.

Payments made by BPAY are not external transfers and have their own terms and conditions.

In addition to the terms and conditions of Internet Banking (above), the following terms and conditions apply to external payments:

- You must correctly input the payees account number and BSB, and payees account name.
- we will not cross check or verify payee account details.
- The receiving ADI will only use BSB and account number to process payments. Account names are not cross checked against the BSB or account number and if you provide us with an incorrect BSB or account number, funds may be sent to the wrong account and it may not be possible to recover funds from an unintended recipient
- Payments made on weekends, public holidays or after 4pm on a business day will be sent on the next business day.
- We are not liable for any delays or errors by other parties, such as the failure of the receiving ADI to process the payment in a timely manner.
- We are not liable for any refusal by a Third Party or other Financial Institution to accept or acknowledge receipt of the payment.
- An external transfer cannot be stopped once it has left FSCU. If you did not authorise the transaction please contact us.

You must also carefully read the section on Mistaken Internet Payments.

56. BPAY®

BPAY is an electronic bill payment system which enables payments to be made through Internet Banking, Mobile Banking and at our office. You can pay bills that have the BPAY logo with this service.

We are a member of BPAY. We will tell you if we are no longer a member of BPAY.

56.1 Using BPAY

BPAY can be used to pay bills bearing the BPAY logo as a one off payment, a future dated payment or a regular payment. 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 (found on your bill), the amount to be paid and the account from which the amount is to be paid.

You acknowledge that we are not required to effect a BPAY Payment if you do not give us all the information specified above, or if any of the information you give us is inaccurate.

We will debit the value of each BPAY Payment and any applicable fees to the account from which the relevant BPAY Payment is made.

If you instruct us to make any BPAY Payment, but close the account to be debited before the BPAY Payment is processed, you will 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 and use of BPAY.

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

56.2 Processing of BPAY Payments

A BPAY Payment instruction is irrevocable. Except for future-dated payments, 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.

You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay) when making a BPAY Payment or if you did not authorise a BPAY Payment that has been made from your account.

If we are advised that your payment cannot be processed by a Biller, we will:

- Advise you of this;
- Credit your account with the amount of the BPAY Payment;
- Take all reasonable steps to assist you in making the BPAY Payment as quickly as possible.

56.3 BPAY Mistaken Amounts

You must be careful to ensure you tell us the correct amount you wish to pay. If you make a BPAY Payment and later discover that:

- The amount you paid was greater than the amount you needed to pay, you must contact the Biller to obtain a refund of the excess;
- The amount you paid was less than the amount you needed to pay, you can make another BPAY Payment for the difference between the amount you actually paid and the amount you needed to pay.

56.4 Future Dated BPAY and Internet Payments

You may arrange future dated payments. If you use this option you should be aware that:

- You are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all future dated payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility and if we have agreed that the credit facility may be used for that purpose, there must be sufficient available credit for that purpose.
- If there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY Payment or internet payment will retry for a further five (5) Business Banking days before the payment is considered to be rejected. Once the payment has been rejected five (5) times the payment will automatically be cancelled and you may be charged a dishonour fee if this fee forms part of our Fees and Charges brochure.
- You are responsible for checking your account transaction details or account statement to ensure the future dated payment is made correctly.
- You should contact us if there are any problems with your future dated payment(s).
- You must contact us if you wish to cancel a future dated payment after you have given the direction but before the date of payment. You cannot stop the payment on or after that date.

57. NPP, PayID, NPP International Payments and OSKO

The PayID service enables payers to make NPP Payments to payees using an alternative identifier instead of the payee's 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 institutions support the NPP Payment service;
- the payee's account is able to receive the particular NPP Payment; and
- the PayID is not locked.

For Terms of Use and 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 clause 58.

For your rights in relation to the investigation and recovery of mistaken payments, misdirected payments and unauthorised (including fraudulent) NPP Payments refer to clause 6.

57.1 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.

57.2 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.

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 us to discuss duplicate PayIDs.We cannot disclose details of any personal information in connection with duplicate PayIDs.

57.3 Transferring your PayID

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 App. 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 refer to clause 57.5. 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.

57.4 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.

57.5 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 us.

57.6 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 section 49)

57.7 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.

58. 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.

58.1 How to use Osko

The eligible accounts for linking to Osko Payments are set out in Table in clause 33. 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.

58.2 How Osko Payments work

Osko Payments must be single immediate payments.

58.3 Payment Directions

You must give us the information specified in this clause 58 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.

59. PayTo Terms and Conditions

59.1 Creating a Payment Agreement

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

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

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

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

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

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

59.2 Amending a Payment Agreement

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

We will send you notification/s of proposed amendments to the payment terms of the Payment Agreement requested by the Merchant or Payment Initiator. Such amendments may include variation of the payment amount, where that is specified in the Payment Agreement as a fixed amount, 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 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 Payment Agreement in the Mandate Management Service and the amendment will then be deemed to be effective. If you decline, the amendment will not be made. A declined amendment request will not otherwise affect the Payment Agreement.

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

59.3 Pausing your Payment Agreement

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

Merchants and Payment Initiators may pause and resume their Payment Agreements. If the Merchant or Payment Initiator pauses a Payment Agreement to which you are a party, we will promptly notify you of that, and of any subsequent resumption, via 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 Payment Agreement by the Merchant or Payment Initiator.

59.4 Cancelling your Payment Agreement

You may instruct us to cancel a Payment Agreement on your behalf by y sending us a Secure Mail message via your Internet Banking, Mobile Banking App, or by contacting us. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the cancellation. [You will be liable for any loss that you suffer as a result of the cancellation of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator (for example, any termination notice periods that have not been adhered to).

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

59.5 Migration of Direct Debit arrangements

Merchants and Payment Initiators who have existing Direct Debit arrangements with their customers, may establish Payment Agreements for these, as Migrated DDR Mandates, in order to process payments under those arrangements via the NPP rather than BECS. If you have an existing Direct Debit arrangement with a Merchant or Payment Initiator, you may be notified by them that future payments will be processed from your Account under PayTo. You are entitled to prior written notice of variation of your Direct Debit arrangement and changed processing arrangements, as specified in your Direct Debit Service Agreement, from the Merchant or Payment Initiator. If you do not consent to the variation of the Direct Debit

arrangement you must advise the Merchant or Payment Initiator. We are not obliged to provide notice of a Migrated DDR Mandate to you for you to confirm or decline. We will process instructions received from a Merchant or Payment Initiator on the basis of a Migrated DDR Mandate.

You may amend, pause (and resume) or cancel your Migrated DDR Mandates, or receive notice of amendment, pause or resumption, or cancellation initiated by the Merchant or Payment Initiator, in the manner described in clauses 59.2,59.3 and 59.4.

59.6 Your responsibilities

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

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

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

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

You are responsible for ensuring that you have sufficient funds in your Account to meet the requirements of all your Payment Agreements and Migrated DDR Mandates. Subject to any applicable laws and binding industry codes, we will not be responsible for any loss that you suffer as a result of your Account having insufficient funds. Our general customer terms and conditions, which are available on our website, will apply in relation to circumstances where there are insufficient funds in your Account.

If you receive a Payment Agreement creation request or become aware of payments being processed from your Account that you are not expecting, or experience any other activity that appears suspicious or erroneous, please report such activity to us by calling us on 08 8227 2222.

Use of the facilities that we provide to you in connection with establishing and managing your Payment Agreements and Migrated DDR Mandates is required to meet terms and conditions of their use https://fscu.com.au/.

You are responsible for ensuring that:

a. all data you provide to us or to any Merchant or Payment Initiator that subscribes to PayTo is accurate and up to date;
b. you do not use PayTo to send threatening, harassing or offensive messages to the Merchant, Payment Initiator or any other person; and
c. any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.

59.7 Our responsibilities

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

We may monitor your Payment Agreements or Migrated DDR Mandates for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreement or Migrated DDR Mandate s if we reasonably suspect misuse, fraud or security issues. We will promptly notify you of any such action to pause or cancel your Payment Agreement.

If you become aware of a payment being made from your Account, that is not permitted under the terms of your Payment Agreement or Migrated DDR Mandate or that was not authorised by you, please contact us as soon as possible via by calling 08 8227 2222 and submit a claim. We will not be liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement or Migrated DDR Mandate.

59.8 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.

60. Cards

This section applies if you or any signatory have been issued with, or requested a Visa Debit card to access your Linked Account(s).

Features and Benefits Your card gives you convenient access to your money, when and where you need it. A card may be used for:

- Visa Debit Purchases (and cash withdrawals[1]) at retail outlets within Australia that display the eftpos logo such as supermarkets and petrol stations
- Purchases from any Merchant displaying the Visa logo, both in Australia and overseas
- Visa Debit Purchases and bill payments via the internet, mail or telephone
- Withdrawing cash from ATMs within Australia displaying the Visa logo
- Obtaining your Linked Account balance from ATMs within Australia displaying the Visa logo
- Withdrawing cash from overseas ATMs displaying the Visa Plus logo
- Obtaining your Linked Account balance from overseas ATMs displaying the Visa Plus logo
- Identification purposes when you withdraw or deposit funds at our branches
- Enable roundup[2]

[1]This service is not available at all retail outlets. Limits may be imposed.

[2]Conditions apply, see section63

60.1 Obtaining a Card

You must be 12 years of age or older to obtain a card. Members under 12 years of age may still apply and be issued a card at our discretion.

Upon acceptance of your card application, your card will be ordered and sent to your postal address. When you receive your card you must sign your physical card immediately as a means of preventing fraudulent or unauthorised use of your card. You must ensure that any signatory signs any physical card issued to them immediately upon receiving it. You must activate it and select a PIN via Mobile App or Internet banking, alternatively we will issue you with a PIN, the PIN enables you to complete an electronic transaction. Your new PIN must contain a minimum of four digits and a maximum of six digits. You must not activate your card until you receive it as you may be liable for unauthorised transactions on your card which result from you activating your card prior to receiving it.

If you need assistance to activate the card, call us on 8222 2722 or visit our office. You may be required to provide identification we reasonably require to confirm your identity in order to complete the activation of your card. The Visa Debit card remains the property of FSCU.

60.2 To use your card

Refer to the account descriptions for information on the EFT Access facilities available for each account. You can only use your card to perform transactions on the nominated savings account. Your transactions will not necessarily be processed to your account on the same day.

You should also refer to the Fees and Charges brochure which details fees and charges applicable to transactions.

We will advise you from time to time of the transactions that may be performed using your card.

We will also advise you of the EFT terminals of other Financial Institutions that may be used and your daily combined cash and EFTPOS limit. You should also refer to the Fees and Charges brochure for fees that may apply to your transactions.

You agree that we have the right to decline authorisation for any EFT transaction for any reason. We will not be liable to you or any Third Party for any loss or damage as a result of a declined authorisation.

60.3 Using your Card at a Merchant Terminal

At many retailers, you can use your card at a Merchant Terminal to make a purchase and your money will be drawn directly from your Linked Account. If you are using a Visa Debit card, you can select either 'Savings' or 'Credit'. If you select 'Savings' it will be an eftpos transaction. Alternatively, you can select 'Credit' on the keypad (where this is available). This is a Visa purchase. Depending on the transaction amount, you may or may not be required to enter your PIN. Some retailers may allow you to include 'cash out' when you select 'Credit' or 'Savings' and input your PIN. Some retailers may charge you a fee for this service.

60.4 Using your card with payWave (contactless payments)

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 using payWave, you will need to place your card on or near the merchant's contactless terminal. 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.

PayWave Payments using the contactless functionality can only be made at a participating Merchant Terminal. A Contactless Payment may be processed as either an eftpos transaction or Visa purchase. This is at the discretion of the Merchant. Transaction value limits do apply and, if you exceed these limits, you will still need to enter a PIN.

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

60.5 Using Your Card at an ATM

To guard against fraud, ATMs only allow two incorrect PIN attempts in a 24 hour period. On a third incorrect attempt, your card will be retained by the ATM and further transaction attempts denied. ATMs that don't have the capacity to capture cards will instead freeze your card's access to your Linked Account(s) for a period of 24 hours from the last unsuccessful attempt. Ensure you remove your card from the ATM at the completion of your transaction. Failure to take appropriate care with your card could leave you liable for any unauthorised transactions

60.6 Using the Card outside Australia

All transactions made overseas on the card will be converted into Australian currency by Visa Worldwide, and calculated at a wholesale market rate selected by Visa from within a range of wholesale rates or the government mandated rate that is in effect one day prior to the central processing date (that is, the date on which Visa processes the transaction).

The card can be used to make a purchase or obtain a cash advance (either in a foreign currency or Australian dollars):

- While overseas; or
- In Australia where the Merchant is overseas, or the Financial Institution or entity processing the transaction is located overseas

- In some cases, overseas Merchants may allow you to pay in Australian dollars (for example when making a purchase online or over the phone). This is still considered an international transaction as the transaction is processed overseas. Even though a price may be shown in Australian dollars, the Merchant may still be located overseas or choose to process their payments outside of Australia. It is best to check with the Merchant before you pay if you are unsure.

International Transactions are subject to the International Transaction Fee which is outlined in our Fees and Charges booklet. This Fee will be deducted once the transaction has debited your account and will be itemised separately on your transaction listing.

Some overseas Merchants and EFT terminals charge a surcharge for making an EFT transaction. Once you have confirmed that transaction you will not be able to dispute the surcharge. It may appear on your Statement as part of the purchase price.

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

Before travelling overseas you should:

- Obtain the Card Hotline phone number for Visa International in the country of your destination.
- Let us know your travel plans so we are aware of the potential for changed or unusual spending patterns while you are away and can alert our 24/7 fraud monitoring service.
- Be aware that some overseas Merchants may require your signature to authorise a transaction.
- Be particularly aware to always check your Statement carefully and advise us promptly of any unauthorised transactions.

A cardholder 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 by you to comply with them.

60.7 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 that you should not be issued with a replacement card for the security of us or your account; or
- you have not transacted on your card for a period of 12 months or more.

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

60.8 Digital Card

We may provide you with a digital copy of your card that can be added to Apple Pay, Google Wallet and Samsung Pay and be used for a more selective range of transactions and participating merchants. Registration of your Visa card into a digital wallet is subject to us identifying and verifying you. Once registered, you can make purchases at participating merchants as if the device was a Visa payWave enabled card. The same conditions apply to your transactions using a digital wallet as transactions using your Visa card.

We do not charge for allowing registration of a digital wallet but there may be charges by your telecommunications provider for using the device.

We do not guarantee that a digital wallet will be accepted by all merchants and we are not liable to you for any loss you suffer if a merchant refuses to accept a digital wallet.

To prevent fraudulent or unauthorised use of your linked account, a digital card will be issued with card controls in place to restrict its use. You can change these card controls but must ensure that you maintain the security of your device or account through which your digital card can be viewed or accessed.

There will be additional terms and conditions issued by the digital wallet provider and your telecommunications provider. We are not the provider of the digital wallet and not responsible for its use

and function and questions about its use or problems must be directed to the digital wallet provider. The digital wallet provider is responsible for security breaches affecting information stored in and sent from a digital wallet.

Follow the procedures of the digital wallet provider to remove your Visa card from a digital wallet.

We can block you 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 to protect you or us from a legitimate risk. For example, we may do this if we suspect fraud by you or against you, if you have an overdue or negative balance on your account, if the law changes or we are directed to do so by the digital wallet provider or by the applicable card scheme. We can cease to support digital wallets at any time.

By registering, you agree that we may exchange information about you with the digital wallet provider and the applicable card scheme to enable the use or the improvement of the digital wallet, and providing information to you about your digital wallet transactions.

WARNING: If you add a card to one of your devices and have other devices sharing the same account this may allow your card to be added to the other devices and permit the users of those devices to see card information. Contact your digital wallet provider for more information.

60.9 Security Risks

Unless the proper precautions are taken, there are risks that your card may be lost, stolen or used without your permission. You can update the status of your card to Lost or Stolen within the Mobile Banking App or Internet Banking. There are also inherent risks associated with EFT Transactions. Although we take all precautions, the security of electronically initiated transactions can never be guaranteed. In some circumstances, you may be liable for unauthorised use of your card. You should read these terms and conditions to understand your liability as a result of unauthorised use of the card and ways by which you can minimise the risk of a security breach.

60.10 Using card controls on your Visa Debit card

You must be a FSCU cardholder that is registered for Internet Banking in order to access the card controls service within internet banking and within the FSCU app. You may be able to use card controls in order to do the following:

Function	How the card control service works in Australia	How the card control service works Internationally	Things you should be aware of
ATM withdrawals	Disabling Australian ATM withdrawals on your access card will block cash withdrawals or cash transfers at an Australian ATM.	Disabling International ATM withdrawals on your access card will block cash withdrawals or cash transfers made at an ATM overseas	This won't affect staff assisted or non-ATM self-service cash withdrawals/transfer made on your access card at our office.
Digital wallet	Disabling Australian digital wallet will block the ability to make a payment via Apple Pay, Google Pay and Samsung Pay or any other service we may offer as a mobile payment system (i.e. when you use your phone to Tap & Pay) or any other service we may offer as a digital payment system such as payment via Garmin and Fitbit or via other wearables, at a domestic electronic terminal, inside apps and on websites where the merchant	Disabling International digital wallet will block the ability to make a payment via Apple Pay, Google Pay and Samsung Pay or any other service we may offer as a mobile payment system (i.e. when you use your phone to Tap & Pay) at international electronic terminal, inside apps and on websites where the merchant processes the payment outside Australia.	

	processes the payment within Australia.		
In-store transactions	Disabling Australian in-store transactions on your access card will block transactions made where the physical card is presented at a domestic electronic terminal at the time of processing the transaction (excluding ATMs). This will also decline Australian payWave transactions.	Disabling International in-store transactions on your access card will block transactions made where the card is physically presented at an international electronic terminal at the time of processing the transaction (excluding ATMs). This will also decline International payWave transactions.	This won't affect: • Digital wallet transactions • online transactions
Online transactions	Disabling Australian online transactions on your access card will block transactions processed in Australia where the card is not present. This could include (but is not limited to) online, phone, or mail order transactions where the merchant processes the transaction domestically.	Disabling International online transactions on your access card will block transactions processed by overseas merchants and transactions made in Australia (such as on Australian websites, mail orders and over the phone) where the merchant processes the transaction overseas.	This won't affect purchases made with your access card in store or with payWave
payWave Disabling	Australian payWave transactions on your access card will block transactions made by 'tapping' or 'waving' the card within a small distance of the domestic electronic terminal.	Disabling International payWave transactions on your access card will block transactions made by 'tapping' or 'waving' the card within a small distance of the international electronic terminal.	This won't decline transactions that are made by either inserting or swiping your card. You will also be able to make Digital wallet transactions (i.e. using your phone to tap and pay).

Function	How the card control service works both in Australia and Internationally	Things you should be aware of
Report a Card lost or stolen	By reporting your card lost or stolen, rather than just applying a temporary block, you are irrevocably notifying FSCU that you wish for the card to be cancelled. Once an access card has been reported lost or stolen the same card cannot be reactivated.	A new access card will not automatically be issued to you. A replacement card can be ordered by contacting us on 08 8227 2222, visiting our office or sending us a secure email
Change PIN	This refers to the access card PIN and enables you to change the PIN.	The change occurs immediately.
Temporary Card Block	Blocking your access card enables you to temporarily disable all card control indicators on the card except digital wallet. You may choose to use this card control when you have misplaced your physical card.	Digital wallet transactions will not be blocked unless digital wallet have been set to disable after temporarily blocking your card.

60.11 Additional Cards.

If you have a visa debit card with us, you may authorise us, if we agree, to issue an additional visa card to a signatory on your account. The additional card is usually called a subsidiary card. We will only issue a subsidiary card to a person who is over the age of 18 (unless we agree to a younger age).

Giving somebody a subsidiary card gives the person access to the money in your account, including any credit limit. You will be liable for any money that the subsidiary cardholder withdraws from your account using the subsidiary card.

Each cardholder will be issued with a Card and PIN. You must ensure that each signatory protects their Card and PIN in the same way these Conditions of Use require you to protect your Card and PIN.

You may instruct us to cancel an additional Card at any time.

If you instruct us by telephone or face to face in our office to cancel an additional Card you will not be liable for any losses resulting from unauthorised use of the additional Card following cancellation.

60.12 Recurring Card Payment Arrangements

You can use your Visa Debit card to establish a recurring payment arrangement. These arrangements are not covered by the Direct Debit conditions but are governed by Visa Scheme Rules.

To change or cancel any recurring payment arrangement you should contact the Merchant at least 15 days prior to the next scheduled payment. You should retain a copy of this change or cancellation request.

Until you cancel the recurring payment with the Merchant we are obliged to process the payment**.**

If the Merchant does not comply with your request to cancel the recurring payment you must send us a copy of your cancellation request to enable us to dispute the ongoing payment on your behalf under the chargeback provisions below.

Should your card details change (e.g. lost, stolen, expired) or your account is closed then you must request the Merchant to change the details of your recurring payment. If you fail to do so your recurring payment may not be honoured and the Merchant may no longer provide the goods or services.

60.13 Disputing a Card Transaction (Chargeback)

A chargeback is a right that we exercise on behalf of a member holding a card (the cardholder). It is a right to, in certain circumstances, seek, on your behalf, the reversal of a transaction (" a charge back") and its debiting to the merchant's account and its financial institution. If you dispute a card transaction we will promptly claim a chargeback right on your behalf for the most appropriate reason where one exists. If a card transaction was:

- unauthorised,
- for goods or services that the Merchant did not deliver,
- for goods and services which did not match the description provided by the Merchant,
- unauthorised payments debited to your card pursuant to a recurring payment arrangement (i.e. where payments continue to be debited even though the recurring payment arrangement has been cancelled)

A Chargeback right will only be possible in respect of a Purchase which involves the use of a user's card details.

You should make every effort to report a disputed transaction to us in writing within 30 days of the date of the statement of account which itemises the disputed transaction, so that we may reasonably ask for a chargeback where such right exists. A failure to report a disputed transaction and/or provide additional information within this timeframe and in the form we require could affect our ability to claim a chargeback right (if any) under the Card Scheme Rules.

If you dispute a transaction with us within the required timeframe and a chargeback right exists under the Card Scheme Rules, we will claim a chargeback on your behalf without delay. We will also:

- ensure we claim the chargeback for the most appropriate reason; and

- not accept a refusal to chargeback by the Merchant's financial institution unless it is reasonable and consistent with the Card Scheme Rules.

Where possible, we will assist you to seek a chargeback of any unauthorised transaction debited to your account under a regular payment arrangement where payments continue to be debited because the Merchant has not complied with a user's request to cancel the arrangement.

You are not able to reverse a transaction authenticated by Visa Secure unless we are liable under the ePayment Code.

60.14 Use after cancellation or expiry of a card

You must not use your Visa Debit card:

- after the valid date shown on the face of the Visa Debit card, or
- after the Visa Debit Card has been cancelled.

You will continue to be liable to reimburse us for any indebtedness incurred through such use whether or not you have closed your account.

60.15 Exclusions of Warranties and Representations

We do not warrant that Merchants or EFT terminals displaying the Visa or eftpos logo or promotional material will accept the Visa Debit card.

We do not accept any responsibility should a Merchant, Financial Institution, EFT Terminal or other institution displaying Visa or eftpos signs or promotional material refuse to accept or honour the card.

We are not responsible for any defects in the goods and services you acquire through the use of the Visa Debit Card. Any complaints about goods and services must be addressed with the Merchant.

61. Account Detail Changes

From time to time we may inform you of what other information may be viewed when using the Internet Banking Facility and what other changes you may be able to effect to that information via the Internet Banking Facility. If we give you access to make changes via the Internet Banking Facility, you agree that effective from the time you confirm the changes, by submitting them to us via the Internet Banking Facility, you are responsible and liable for any changes made via the Internet Banking Facility. Access to make changes will not be available where two or more signatures are required for account operations.

62. Cancellation of Access Services

You may request to cancel your Visa Debit card, or access to Internet Banking, BPAY, or Mobile banking in person or over the phone.

We may suspend or cancel your access to Visa Debit card or access to Internet Banking, BPAY or Mobile Banking at any time for security reasons or if:

- you breach these Terms and Conditions or you, or
- we reasonably suspect that you or someone acting on your behalf, is being fraudulent.
- we reasonably suspect that your account or access method has been compromised or is at risk of being compromised

We may cancel your access to Visa Debit card, or access to Internet Banking, BPAY, or Mobile Banking, acting reasonably, by giving you (30) days' notice. The notice does not have to specify the reasons for cancellation.

We may suspend your access to the Internet Banking service, for security reasons if you have not accessed it within a 6 month period.

If, despite cancellation of your access, you carry out transactions using Internet Banking, BPAY, or Mobile Banking, you will remain liable for that EFT transaction.

We may not reissue your Visa Debit card if you have not used your card within 6 months of its expiry date.

In the case of Visa Debit card you will be liable for any transactions you make using your card before they are cancelled but which are not posted to your account till after cancellation of the card. We may demand return or destruction of your Visa Debit card.

Your access to Visa Debit card, or access to Internet Banking, BPAY or Mobile Banking will be terminated when:

- We notify you that your access or the account with us has been cancelled;
- You close the last of your accounts with us which has access to the facilities;
- You cease to be a member; or
- You alter the authorities governing the use of your account with access to these facilities (unless we agree otherwise

63. Round UP

Round up offers an easy way to set up automatic debits of small amounts from one account and the credit that same amount into a secondary account, usually a savings account.

Once activated, each time an eligible purchase is made with a Visa debit card (including when information from a card is used), the purchase amount is rounded up to the nearest dollar and the 'round up' amount is transferred to the secondary account.

Example: You select to round up to the nearest $1. You make a purchase costing $9.50 with your Visa debit card. When your account is debited for the purchase amount we'll also automatically transfer 50 cents from your account to your nominated savings account.

Once you have activated Round UP, every time a debit transaction is made in-store, payWave, digital wallet, international or online with your visa debit card the difference between the purchase amount and the nearest $1, $5, $10 (rounded up) is transferred into your nominated savings account.

The round up amount will not occur if the funds are not available in your nominated account.

Accounts eligible for round up are detailed in the Summary of Accounts & Access Facilities.

You can cancel round up at any time via your FSCU app.

64. Spend Tracker

'Spend Tracker' allows you to track cleared payments from eligible accounts in the FSCU app. This includes card transactions made in person, online or over the phone, mobile wallet transactions (such as Apple Pay or Google Pay), recurring transactions, Pay Anyone payments, BPAY® payments, direct debits, PayTo transactions, international money transfers and fees or charges on your account.

Spend Tracker is only an indicator of your spending and will not restrict your spending or saving that is linked to your FSCU accounts.

65. Telegraphic Transfers

FSCU provides outward and inward telegraphic transfer services to our members through our business partner Convera Australia Pty Ltd trading as Convera ACN 150 129 749; AFSL 404092. All telegraphic transfers you initiate through FSCU will be sent to beneficiaries account via Convera. Fees & charges and terms & conditions apply.

Inward Telegraphic Transfers Funds forwarded from outside of Australia may pass through other financial institutions before being credited to your FSCU account. Each institution involved in the transfer process may deduct a processing fee from the amount being remitted before on-forwarding the funds. FSCU will pass on any fee charged by other financial institutions involved in the transfer. We will credit telegraphic transfer funds to your account within 1 to 2 business days once the payment has been received by FSCU. Provided all information supplied on the request is complete and correct, funds transferred from major overseas currencies generally take 3-5 business days to be received, however this is an estimate only and cannot be guaranteed. Funds transferred from minor overseas currencies generally take 7-10 working days, however

this is an estimate only and cannot be guaranteed. The conversion of foreign amounts into Australian Dollars is performed by our international payments provider before the funds are received at FSCU for processing.

Outward Telegraphic Transfers Requests to transfer funds via telegraphic transfer will be processed within 1-2 business days. Telegraphic transfers are manually processed and will pass through at least one, and up to four other institutions before being credited to the receiving account. Please be aware that all international money transfers are monitored by government agencies for the purpose of detecting terrorist and criminal activity. For this reason and the possibility of incorrect information being provided when remitting funds, our international payments provider may require further information or details from you before the international transfer can be processed, and you agree that all information may be passed on by Convera to third parties as appropriate Provided all information supplied on the request is complete and correct, funds transferred to major overseas currencies generally take 3-5 business days to be received, however this is an estimate only and cannot be guaranteed. Funds transferred to minor overseas currencies generally take 7-10 working days, however this is an estimate only and cannot be guaranteed. Each institution involved in the transfer process may deduct a processing fee from the amount being remitted before on-forwarding the funds. FSCU cannot lodge a trace on international telegraphic transfers until 5 business days after telegraphic transfer has been lodged. You are responsible for the completeness and accuracy of the details you provide to us in relation to a telegraphic transfer.

We are not responsible to you or a beneficiary for any direct or consequential loss as a result of:

- any error or omission in the details you provide when requesting a telegraphic transfer
- any error, omission or negligence of Convera or
- any delay in payment to the Beneficiary, other than loss due to our negligence or in relation to any breach of a condition or warranty implied by the law of contracts for the supply of goods or services which may not be excluded, restricted or modified at all, or only to a limited extent.

Contacting Fire Service Credit Union

Phone: (08) 8227 2222
Fax: (08) 8227 2422
Email: fscuhelpdesk@fscu.com.au
Website: www.fscu.com.au
Mail: Level 1, 22 Chancery Lane, Adelaide

Office Hours

Monday to Friday	**8.30am – 4.45pm**
Tuesday	**9.30am – 4.45pm**

Fire Service Credit Union Ltd
ABN 17 087 651 152
AFSL and Australian Credit Licence 237515