COMMUNITY FIRST CREDIT UNION LTD ACCOUNT & ACCESS FACILITY

Terms and Conditions

Incorporating Customer Terms for Osko

This document must be read together with the *Summary of Accounts, Availability of Access Facilities & Transaction Limits* brochure and the *Fees & Charges* brochure. Together these brochures form the Conditions of Use for the Community First Credit Union Account and Access Facility.

Date taking effect: 18 November 2019

The Community First Credit Union Account and Access Facility is issued by:
Community First Credit Union Ltd
ABN 80 087 649 938
Australian Financial Services Licence 231204

Please note that by opening an account or using an access facility you become bound by these conditions of use.

Please keep these Conditions of Use in a safe place so you can refer to it when needed. Alternatively, you can obtain information set out in this document [and download this document] by visiting our website at www.communityfirst.com.au

How To Contact Us

Visit us at any of our stores – visit our website at www.communityfirst.com.au for our store details

	Telephone:	Community First Direct on 1300 13 22 77
	Mail:	PO Box 98, Lidcombe NSW 1825
	Email:	askus@communityfirst.com.au
	Fax:	(02) 9735 1661

To report the loss, theft or unauthorised use of your Visa Card or wearable device

- **in Australia**

  call the Visa Card Hotline on 1800 648 027 (Australia wide toll free), 24 hours a day, everyday. Please also contact us to report the loss, theft or unauthorised use.
- **overseas – for VISA**

  Please contact us before you travel overseas for the current VISA hotline arrangements

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

Codes Of Conduct

We warrant that we will comply with the ePayments Code where that Code applies.

The Customer Owned Banking Code of Practice will apply to you if you are an individual or small business.

Please note that you can obtain a copy of the Customer Owned Banking Code of Practice on request or download it from our website www.communityfirst.com.au

Privacy

We have privacy information contained on our website www.communityfirst.com.au that sets out:

- our obligations regarding the confidentiality of your personal information; and
- how we manage your personal information.

We will give you the privacy information statement whenever we request personal information from you. It is always available on request.

Financial Difficulty

If you ever experience financial difficulty you should inform us promptly. The earlier you do so the sooner we can assist you with your difficulties.

Financial Claims Scheme

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

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

TABLE OF CONTENTS

ACCOUNT OPERATIONS

WHAT IS THE COMMUNITY FIRST CREDIT UNION ACCOUNT AND ACCESS FACILITY?

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

- **Visa Card or wearable device**
- **member chequing**
- **BPAY® (registered to BPay Pty Ltd ABN 69 079 137 518)**
- **Osko Payments**
- **telephone and internet banking**
- **EFTPOS and ATM access**
- **direct debit requests**
- **periodical payments**
- **Bank@Post**

Please refer to the *Summary of Accounts, Availability of Access Facilities & Transaction Limits* brochure for available account types, the conditions applying to each account type and the access methods attaching to each account type.

HOW DO I OPEN AN ACCOUNT?

You will need to become a shareholding member of the Credit Union before we can issue the Community First Credit Union Account and Access Facility to you. To become a member, you will need to:

- **complete a membership application form; and**
- **subscribe for a member share in the Credit Union.**

Proof Of Identity Required

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

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

- **a State or Territory drivers licence or proof of age card**
- **an Australian current passport or one that has expired within the last 2 years;**
- **a photo drivers licence issued by a foreign government;**
- **a passport issued by a foreign government, the United Nations or a UN agency;**
- **a national ID card, with photo and signature, issued by a foreign government, the United Nations or a UN agency.**

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

The law does not allow you to open an account using an alias. An alias is any name other than a name you are commonly known by. If you are commonly known by more than one name you must give us all the names that you are commonly known by.

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

WHAT ACCOUNTS CAN I OPEN?

When we issue you with the Community First Credit Union Account and Access Facility, you have access to the S7 Access Account. You can then activate other accounts as needed. But first check the *Summary of Accounts, Availability of Access Facilities & Transaction Limits* brochure for the different account types available, any special conditions for opening, and the features and benefits of each account type.

WHAT FEES AND CHARGES ARE THERE?

Please refer to the *Fees and Charges* brochure for our current fees and charges, including government fees and charges. We can vary fees or charges from time to time. Please see Notifying Changes on page 13 for details of how and when we must notify you of these changes.

We will also debit your primary operating account for all applicable government taxes and charges unless you request otherwise or you open a McGrath Debit account which will have any fees charged directly to that account.

WHAT INTEREST CAN I EARN ON MY ACCOUNT?

Please refer to our Interest Rates brochure for the current deposit and savings interest rates payable.
We calculate and credit interest to your account as set out in the *Summary of Accounts, Availability of Access Facilities & Transaction Limits* brochure. We may vary deposit or savings interest rates from time to time. However, interest rates on term deposits remain fixed for the agreed term of the deposit. You can obtain information about current deposit and savings interest rates from us at any time or by visiting our website.

WHAT ARE THE TAXATION CONSEQUENCES?

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

When you apply for the Community First Credit Union Account and Access Facility we will ask you for your Tax File Number or exemption. We apply your Tax File Number to each account in the Community First Credit Union Account and Access Facility. You are not obliged to disclose your Tax File Number to us. However, if you do not, we are obliged to deduct withholding tax from any interest you earn at the highest marginal rate.

For a joint account, all holders must quote their Tax File Numbers and/or exemptions, otherwise withholding tax applies to the whole of the interest earned on the joint account.

The deduction of withholding tax will form part of your normal income tax, just as when your employer deducts tax from your salary or wages. When you fill out your tax return, including your interest earned along with your regular income, you may claim the withholding tax paid on the interest as tax already paid together with the tax your employer deducts from your salary or wages.

If you give us your income tax file number, we will not deduct withholding tax on interest that you earn on your account. However, you will still be required to disclose interest as income when you complete your tax return at the end of the financial year.

For business accounts and charities, you need only quote your ABN instead of your Tax File Number.

JOINT ACCOUNTS

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

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

You can operate a joint account on an 'all to sign' or 'either/or to sign' basis:

- 'all to sign' means all joint holders must sign withdrawal forms, cheques, etc
- 'either/or to sign' means any one joint holder can sign withdrawal slips, cheques, etc.

All joint account holders must consent to the joint account being operated on an 'either/or to sign' basis. However, any one joint account holder can cancel this arrangement, making it 'all to sign'.

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

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

TRUST ACCOUNTS

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

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

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

THIRD PARTY ACCESS

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

An authorised person operates on all the accounts you have nominated them to have access to under the Credit Union Account and Access Facility. You are responsible for all transactions your authorised person carries out on your account. **You should ensure that the person you authorise to operate on your account is a person you trust fully.**

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

MAKING DEPOSITS TO THE ACCOUNT

You can make deposits to the account:

- **by cash or cheque at any store**
- **by direct credit e.g. from your employer for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the direct credit**
- **by transfer from another account with us**
- **by transfer from another financial institution**
- **by cash or cheque at selected ATMs, if your account is linked to a Visa Card: See ePayments Conditions of Use: Section 1**

- **via Bank@Post,**

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

DEPOSITS USING ELECTRONIC EQUIPMENT

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

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

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

DEPOSITING CHEQUES

You can only access the proceeds of a cheque when it has cleared.

WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT

You can make withdrawals from the account:

- **over the counter at any store**
- **by direct debit**
- **by member cheque, if your account is linked to a member cheque book**
- **by telephone or internet banking**
- **by BPAY® and Osko®**
- **at selected ATMs, if your account is linked to a Visa Card**
- **via selected EFTPOS terminals, if your account is linked to a Visa Card or wearable device (note that merchants may impose restrictions on withdrawing cash)**
- **via Bank@Post.**

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

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

DEBITING TRANSACTIONS GENERALLY

We will debit transactions received on any one day in the order we determine in our absolute discretion. Transactions will not necessarily be processed to your account on the same day.

We have the right to decline to accept your authorisation for any transaction if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give the authorisation. We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result of our action.

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

OVER THE COUNTER WITHDRAWALS

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

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

WITHDRAWALS USING OUR CORPORATE CHEQUES

This is a cheque the Credit Union draws payable to the person you nominate. You can purchase a corporate cheque from us for a fee: see the *Fees & Charges* brochure.

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

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

TRANSACTION LIMITS

We limit the amount of daily withdrawals or payments you may make using electronic methods, either generally or in relation to a particular facility. These transaction limits are set out in the *Summary of Accounts, Availability of Access Facilities & Transaction Limits* brochure.

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

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

OVERDRAWING AN ACCOUNT

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

Alternatively, we can honour the transaction and overdraw your account. We may charge you:

- **interest at our current overdraft rate, calculated on the daily closing balance, and/or**
- **A fee for each member cheque or direct debit presented whilst your account has insufficient cleared funds: see the *Fees & Charges* brochure,**
- **A fee where your account has remained overdrawn or overlimit for 1 day or more during a calendar month: see the *Fees & Charges* brochure.**

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

SWEEP FACILITY

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

ACCOUNT STATEMENTS

We will send you account statements at least every 4 months. You can ask us for an account statement at any time. We may charge a fee for providing additional statements or copies: see the *Fees & Charges* brochure.

When you become a member of Community First Credit Union and you provide a valid email address, we will give you the option of registering for our e-statements service and will do so where you provide us with a valid e-mail address. Paper statements may be requested at any time by contacting us.

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

E-STATEMENTS

By providing your e-mail address you agree to our terms and conditions for e-statements

Community First Credit Union's statement service allows us to provide you statements for your savings, term deposit, loan and credit card accounts using electronic means. When you become a member of Community First Credit Union and you provide a valid email address, we will automatically register you for our e-statements service as the default statement delivery method. Once registered for this service, you will receive an email at your nominated email address when an E-Statement is available online via our secure site. To view, save and print E-Statements you will need to have Acrobat reader version 4.0 (or higher).

When you are registered for E-Statements:
You will not receive paper statements;
You can elect to receive paper statements at any time instead by contacting us on 1300 13 22 77 or visiting your nearest Community First Financial Services Store ;
you are required to keep your email address details with us up to date, and;
you should check your email regularly for notices that E-Statements are available

Your registration to receive E-Statements takes effect at the Membership level. Therefore, statements for all accounts under your Membership will be available electronically. Selection of statement type must be applied for all accounts under your membership. I.e. it is not possible to select E-Statements for some accounts and paper statements for other accounts.

E-Statements will be available online for at least six months from the date that you are notified that an E-Statement is available. You should print or save your E-Statements if you require a copy for taxation or other purposes. Fees may apply if you request a copy of a statement from us (please refer to the Fees and Charges Schedule available from www.communityfirst.com.au).

Consent to receive E-Statements

I agree:
1. to receive my statements electronically, satisfying any legal obligations for Community First to provide statements;
2. to be notified of the availability of statements by email to the nominated email address provided at the time of registration for this service;
3. that I have the option at any time to revert to receiving paper statements;
4. that Community First Credit Union is not liable for misuse or access of this service by any other person;
5. that an E-Statement is deemed to have been received by me if a notification that I have a statement is sent to my server at the nominated email address, whether or not I choose to access my email;
6. that E-Statements are taken to be received on the day that the notification email enters the information system of my internet service provider or the host of the nominated email address;
7. that a statement will not be deemed to have been received by me if Community First Credit Union receives notification that my mailbox is full; or I cannot receive an email notification (due to no fault of my own); or an email notification to me is returned to Community First Credit Union undelivered;
8. to promptly advise Community First of any changes in email address or update in nominated email address; and

9. to have and maintain Acrobat reader version 4.0 (or higher) for viewing, saving and printing statements.

Passwords
Your password for E-Statements access should be a minimum of 6 characters in length. We recommend you choose passwords that would be difficult to guess even to people that know you. You should also avoid doing your internet banking at public computers (libraries or internet cafes) and beware of free websites and downloads as they can install harmful programs without you knowing. We recommend you change your password on a regular basis and you install software to protect your computer from viruses and keep it up to date.

WHAT HAPPENS IF I CHANGE MY NAME OR ADDRESS?

If you change your name or address, please let us know immediately.

INACTIVE ACCOUNTS

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

Once your account becomes inactive, we may charge an inactive fee.

DORMANT ACCOUNTS

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

Once your membership becomes dormant, we may:

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

If your account remains dormant for 7 years, we have a legal obligation to remit balances exceeding $500 to the Australian Securities and Investments Commission as unclaimed money.

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 Community First from time to time.

We reserve the right to transfer funds from one of your Community First accounts to another, where the accounts are held in the same name. This may be necessary if, for example, one of your accounts becomes overdrawn, or in payment of any amount overdue on any loan account in the samename.

However, this transfer of funds will not occur where we know that the funds are not held in the same capacity. Further, where we are bound by a specific code, there may be limits on the extent to which funds from your various accounts may be transferred.

Consistent with the Customer Owned Banking Code of Practice, we will, where possible, promptly advise you if it has been necessary to transfer funds between your accounts. However, we are under no obligation to tell you of our intentions prior to transferring funds between your accounts.

NOTIFYING CHANGES

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

Type of change	Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Reducing the number of fee-free transactions permitted on your account	20 days
Changing the minimum balance to which an account keeping fee applies	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited to your account	20 days
Increasing your liability for losses relating to ePayments (see the ePayments Conditions of Use on page 15 for a list of ePayments)	20 days
Imposing, removing or changing any periodic transaction limit	20 days
Changing any other term or condition	when we next communicate with you

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

- notification by letter;
- notification on or with your next statement of account;
- notification on or with the next newsletter;
- advertisements in the local or national media;
- notification on our website.

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

CLOSING ACCOUNTS AND CANCELLING ACCESS FACILITIES

You can close the Community First Credit Union Account and Access Facility at any time. However, you will have to surrender your member cheque book and any access card or wearable device at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding cheque, EFT transactions and fees, if applicable.

You can cancel any access facility on request at any time. However, for direct debit:

- **you can contact your biller or us to cancel any direct debit authority you have given to a biller;**
- **you have to give us 3 business days notice to cancel any direct debit authority you give us.**

We can:

- **close the Community First Credit Union Account and Access Facility in our absolute discretion by giving you reasonable notice and paying you the balance of your account; or**
- **cancel any access facility for security reasons or if you breach these Conditions of Use.**

NOTICES AND ELECTRONIC COMMUNICATION

We may send you notices and statements:

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

We will only use fax or email if the law permits and you have nominated a fax number or electronic address for this purpose. We may also send you notices and statements by some other way that you have agreed to.

If you agree, we may, instead of sending you a notice or statement, post notices or statements to our website for you to retrieve. However, we have to tell you promptly, via email, that the information is available for you to retrieve.

You can vary your nominated email address at any time or cancel arrangements to receive notices or statements by email or by retrieval from our website.

COMPLAINTS

We have a dispute resolution system to deal with any complaints you may have in relation to The Community First Credit Union Account and Access Facility or transactions on the account. Our dispute resolution policy requires us to deal with any complaint efficiently, speedily and sympathetically. If you are not satisfied with the way in which we resolve your complaint, or if we do not respond speedily, you may refer the complaint to our external dispute resolution centre.

If you want to make a complaint, contact our staff at any store and tell them that you want to make a complaint. Our staff have a duty to deal with your complaint under our dispute resolution policy. Our staff must also advise you about our complaint handling process and the timetable for handling your complaint. We also have an easy to read guide to our dispute resolution system available to you on request.

MEMBER CHEQUING

Member chequing is a facility which allows you to make payments by cheque. Under our member chequing facility, we issue you with a cheque book and authorise you to draw cheques on our account at the National Australia Bank. We will debit your account for the value of cheques you draw.

If you have insufficient funds in your nominated account, we may instruct the National Australia Bank to dishonour your cheque. However, we have a discretion to allow the cheque to be paid and to overdraw your account for this purpose. If you overdraw your account, we will charge you interest and fees. Please refer to the section Overdrawing An Account on page 9.

We may not give you access to member chequing if your banking history with the Credit Union is not satisfactory, or if you are under 18.

DIRECT DEBIT

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

To cancel the DDR Service Agreement, you can contact either the biller or us. If you contact us, we will promptly process your instruction to cancel the biller's authority. However, we suggest that you also contact the biller.

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

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

You can also provide us with direct debit instructions yourself to make periodical payments from your account. You must give us at least 3 business days' notice in writing to stop any direct debit you have instructed us to make.

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

PAYPAL

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

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

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

ELECTRONIC ACCESS FACILITIES AND EPAYMENTS CONDITIONS OF USE

Section 1. INFORMATION ABOUT OUR EPAYMENT FACILITIES

You should follow the guidelines in the box below to protect against unauthorised use of your access card, wearable device and pass code. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised epayments. Liability for such transactions will be determined in accordance with the ePayments Conditions of Use and the ePayments Code.

Important Information You Need to Know Before Using a Device to Make Electronic Payments

- **Sign the access card as soon as you receive it.**
- **Familiarise yourself with your obligations to keep your access card, wearable device and pass codes secure.**
- **Familiarise yourself with the steps you have to take to report loss or theft of your access card or wearable device or to report unauthorised use of your access card or wearable device, BPAY® or telephone or internet banking.**
- **If you change a pass code, do not select a pass code which represents your birth date or a recognisable part of your name.**
- **Never write the pass code on the access card or wearable device.**
- **Never write the pass code PIN on anything which is kept with or near the access card or wearable device.**
- **Never lend the access card or wearable device to anybody.**
- **Never tell or show the pass code to another person.**
- **Never tell or show the entire card number nor the card security number (located on the rear of the card in the signature panel) to another person unless you are conducting a card transaction through a secure website or telephone payment service and the merchant payment authorisation requires it.**
- **Use care to prevent anyone seeing the pass code being entered on a device.**
- **Keep a record of the VISA card number and the VISA Card Hotline 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 telephone banking or internet banking service only using the OFFICIAL phone numbers and URL addresses.**
- **If accessing internet banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history.**
- **ALWAYS REJECT any request to provide or to confirm details of your pass code. We will NEVER ask you to provide us with these details.**

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

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

1. Visa Card
2. Wearable device
3. BPAY®
3. Internet Banking
4. Telephone Banking
5. Osko Payments

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

Visa Card or wearable device

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

- **check your account balances;**
- **withdraw cash from your account;**
- **transfer money between accounts;**
- **deposit cash or cheques into your account (at select ATMs only).**

We may choose not to give you a Visa Card or wearable device if your banking history with the Credit Union is not satisfactory or if you are under 12 years of age.

Important Information about Chargebacks for VISA

If you believe a Visa Card or wearable device transaction was:

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

then you can ask us to 'chargeback' the transaction, by reversing the payment to the merchant's financial institution. You can do so by telling us within 30 days after the date of the statement that shows the transaction and providing us with any information we may require.

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

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

Digital Wallet

You may load your Visa Card on to your mobile phone in a digital wallet app. Use of the Visa Card details, via the digital wallet, is governed by these Conditions of Use.

The Digital Wallet Provider is responsible for the functioning of the Digital Wallet, not us.

When you load the Card into Digital Wallet, there is a sharing of your personal information between us and the Digital Wallet Provider and between you and the Digital Wallet Provider.

Important Information You Need To Know When Using Your Digital Wallet On a Mobile Phone

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

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

Our Conditions of Use require you to report these events to us immediately:

- **if your Device has been lost or stolen**
- **you believe your security credentials have been compromised**
- **if you believe there are errors**
- **if you suspect fraud associated with your Digital Wallet**

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

Section 2. DEFINITIONS

(a) **access card** means, our Visa debit card or credit card

(b) **ATM** means automatic teller machine

(c) **business day** means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned

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

- (i) ATM card
- (ii) debit card or credit card
- (iii) wearable device
- (iv) token issued by a subscriber that generates a pass code

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

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

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

- (i) knows but is not required to keep secret, and
- (ii) must provide to perform a transaction

Examples include an account number or member number.

(h) **manual signature** means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet

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

- (i) personal identification number (PIN)
- (ii) internet banking password
- (iii) telephone banking password
- (iv) code generated by a security token.

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

- (v) Osko Payments smart address (PayID)

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

(k) **transaction** means a transaction to which these ePayments Conditions of Use apply, as set out in Section 3.

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

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

(i) a third party signatory to your account

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

(n) **we**, **us**, or **our** means Community First Credit Union

(o) **wearable device** means a near field communication enabled payment device (other than a mobile device or card) including without limitation a wristband, ring or other device we give to a user that is used to perform a transaction.

(p) **you** means the person or persons in whose name this Account and Access Facility is held.

Section 3. TRANSACTIONS

1. These ePayments Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:
   (a) initiated using electronic equipment, and
   (b) not intended to be authenticated by comparing a manual signature with a specimen signature.
2. These ePayments Conditions of Use apply to the following transactions:
   (a) electronic transactions using a device, including ATM, EFTPOS, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature
   (b) telephone banking and bill payment transactions
   (c) internet banking transactions, including 'Pay Anyone'
   (d) online transactions performed using a card number and expiry date
   (e) online bill payments (including BPAY)
   (f) direct debits
   (g) transactions using mobile devices
   (h) Osko Payments.

Section 4. WHEN YOU ARE NOT LIABLE FOR LOSS

1. You are not liable for loss arising from an unauthorised transaction if the cause of the loss is any of the following:
   (a) fraud or negligence by our employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent
   (b) a device, identifier or pass code which is forged, faulty, expired or cancelled
   (c) a transaction requiring the use of a device and/or pass code that occurred before the user received the device and/or pass code (including a reissued device and/or pass code)
   (d) a transaction being incorrectly debited more than once to the same facility
   (e) an unauthorised transaction performed after we have been informed that a device has been misused, lost or stolen, or the security of a pass code has been breached.
2. You are not liable for loss arising from an unauthorised transaction that can be made using an identifier without a pass code or device. Where a transaction can be made using a device, or a device and an identifier, but does not require a pass code, you are liable only if the user unreasonably delays reporting the loss or theft of the device.

3. You are not liable for loss arising from an unauthorised transaction where it is clear that a user has not contributed to the loss.
4. In a dispute about whether a user received a device or pass code:
   (a) there is a presumption that the user did not receive it, unless we can prove that the user did receive it
   (b) we can prove that a user received a device or pass code by obtaining an acknowledgement of receipt from the user
   (c) we may not rely on proof of delivery to a user's correct mailing or electronic address as proof that the user received the device or pass code.

Section 5. WHEN YOU ARE LIABLE FOR LOSS

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

   you are liable under clause 5.2 only if we also prove on the balance of probability that the breach of the pass code security requirements under Section 6 was more than 50% responsible for the losses, when assessed together with all the contributing causes.
4. You are liable for losses arising from unauthorised transactions that occur because a user contributed to losses by leaving a card in an ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.

   Note: Reasonable safety standards that mitigate the risk of a card being left in an ATM include ATMs that capture cards that are not removed after a reasonable time and ATMs that require a user to swipe and then remove a card in order to commence a transaction.
5. Where we can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a device, or that the security of all pass codes has been breached, you:
   (a) are liable for the actual losses that occur between:
      (i) when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and
      (ii) when the security compromise was reported to us
   (b) are not liable for any portion of the losses:
      (i) incurred on any one day that exceeds any applicable daily transaction limit
      (ii) incurred in any period that exceeds any applicable periodic transaction limit
      (iii) that exceeds the balance on the facility, including any pre-arranged credit
      (iv) incurred on any facility that we and you had not agreed could be accessed using the device and/or pass code used to perform the transaction.

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

6. Where a pass code was required to perform an unauthorised transaction, and clauses 5.2 – 5.5 do not apply, you are liable for the least of:
   (a) $150, or a lower figure determined by us
   (b) the balance of the facility or facilities which we and you have agreed can be accessed using the device and/or pass code, including any prearranged credit
   (c) the actual loss at the time that the misuse, loss or theft of a device or breach of pass code security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.
7. In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under clauses 5.2 and 5.5:
   (a) we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring
   (b) the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in Section 6
   (c) the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example, the number and expiry date of a device) is not relevant to a user's liability.
8. If a user reports an unauthorised transaction on a credit card account, debit card account or charge card account we will not hold you liable for losses under Section 5 for an amount greater than your liability if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights).

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

Section 6. PASS CODE SECURITY REQUIREMENTS

1. Section 6 applies where one or more pass codes are needed to perform a transaction.
2. A user must not:
   (a) voluntarily disclose one or more pass codes to anyone, including a family member or friend
   (b) where a device is also needed to perform a transaction, write or record pass code(s) on a device, or keep a record of the pass code(s) on anything:
      (i) carried with a device
      (ii) liable to loss or theft simultaneously with a device

   unless the user makes a reasonable attempt to protect the security of the pass code
   (c) where a device is not needed to perform a transaction, keep a written record of all pass codes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the pass code(s).
3. For the purpose of clauses 6.2(b)–6.2(c), a reasonable attempt to protect the security of a pass code record includes making any reasonable attempt to disguise the pass code within the record, or prevent unauthorised access to the pass code record, including by:
   (a) hiding or disguising the pass code record among other records
   (b) hiding or disguising the pass code record in a place where a pass code record would not be expected to be found
   (c) keeping a record of the pass code record in a securely locked container
   (d) preventing unauthorised access to an electronically stored record of the pass code record.

   This list is not exhaustive.

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

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

   Note 2: For the obligations applying to the selection of a pass code by a user, see clause 6.5.

5. A user must not select a numeric pass code that represents their birth date, or an alphabetical pass code that is a recognisable part of their name, if we have:
   (a) specifically instructed the user not to do so
   (b) warned the user of the consequences of doing so.
6. The onus is on us to prove, on the balance of probability, that we have complied with clause 6.5.
7. Where we expressly authorise particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the pass code security requirements in Section 6.
8. Where we expressly or implicitly promote, endorse or authorise the use of a service for accessing a facility (for example, by hosting an access service on our electronic address), a user who discloses, records or stores a pass code that is required or recommended for the purpose of using the service does not breach the pass code security requirements in section 6.

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

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

Section 8. NETWORK ARRANGEMENTS

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

Section 9. MISTAKEN INTERNET PAYMENTS

1. In this Section 9:
   (a) **direct entry** means a direct debit or direct credit
   (b) **mistaken internet payment** means a payment by a user through a 'Pay Anyone' internet banking facility and processed by an ADI through direct entry where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:
      (i) the user's error, or

(ii) the user being advised of the wrong BSB number and/or identifier.

This does not include payments made using BPAY.

(c) **receiving ADI** means an ADI whose customer has received an internet payment

(d) **unintended recipient** means the recipient of funds as a result of a mistaken internet payment

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

3. If we are satisfied that a mistaken internet payment has occurred, we must send the receiving ADI a request for the return of the funds.

Note: Under the ePayments Code, the receiving ADI must within 5 business days:

(i) acknowledge the request by the sending ADI for the return of funds, and

(ii) advise the sending ADI whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

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

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

6. You may complain to us about how the report is dealt with, including that we and/or the receiving ADI:

(a) are not satisfied that a mistaken internet payment has occurred

(b) have not complied with the processes and timeframes set out in clauses 9.2 – 9.5, or as described in the box below.

7. When we receive a complaint under clause 9.6 we must:

(a) deal with the complaint under our internal dispute resolution procedures

(b) not require you to complain to the receiving ADI.

8. If you are not satisfied with the outcome of a complaint, you are able to complain to our external dispute resolution scheme provider.

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

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

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

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

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

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

➢ **Process where funds are available 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 fromtheir account.**
- **If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder.**
- **The sending ADI must return the funds to the holder as soon as practicable.**

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

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

➢ **Process where funds are not available**

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

Section 10. USING TELEPHONE BANKING AND INTERNET BANKING

1. We do not warrant that:
   (a) the information available to you about your accounts through our home banking service is always up to date;
   (b) you will have 24 hours a day, 7 days per week, access to telephone banking or internet banking.
   (c) data you transmit via telephone banking or internet banking is totally secure.

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

1. If you believe your access card or wearable device has been misused, lost or stolen or the pass code has become known to someone else, you must immediately contact us during business hours or the access card HOTLINE at any time.
   Please refer to How to Contact Us on page 2 for our contact details.

2. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.
3. The access card HOTLINE is available 24 hours a day, 7 days a week.
4. If the access card HOTLINE is not operating when you attempt notification, nevertheless, you must report the loss, theft or unauthorised use to us as soon as possible during business hours. We will be liable for any losses arising because the access card HOTLINE is not operating at the time of attempted notification, provided you report the loss, theft or unauthorised use to us as soon as possible during business hours.
5. If the loss, theft or misuse, occurs OUTSIDE AUSTRALIA you must notify an organisation displaying the VISA sign and also then confirm the loss, theft or misuse of the card or wearable device:
   (a) with us by telephone or priority paid mail as soon as possible; or
   (b) by telephoning the VISA Card Hotline number for the country you are in.

VISA CARD HOTLINE
AUSTRALIA WIDE TOLL FREE
1800 648 027
SYDNEY METROPOLITAN AREA
9959 7480

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

1. If you believe that your pass codes for telephone or internet banking transactions have been misused, lost or stolen, or, where relevant, your pass code has become known to someone else, you must contact us immediately.

   Please refer to How to Contact Us on page 2 for our contact details. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.

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

Section 13. USING THE ACCESS CARD OR WEARABLE DEVICE

1. You agree to sign the access card immediately upon receiving it and before using it as a means of preventing fraudulent or unauthorised use of access card. You must ensure that any other cardholder you authorise also signs their access card immediately upon receiving it and before using it.
2. We will advise you from time totime:
   (a) what transactions may be performed using access card or wearable device;
   (b) what ATMs of other financial institutions may be used; and
   (c) what the daily cash withdrawal limits are.

   Please refer to the *Fees & Charges brochure for details of current transaction limits*
3. You may only use your access card or wearable device to perform transactions on those accounts we permit. We will advise you of the accounts which you may use your access card or wearable device to access.
4. The access card or wearable device always remains our property.

Section 14. USING VISA OUTSIDE AUSTRALIA

1. You agree to reimburse us for any costs, fees or charges of any nature arising out of a failure to comply with any exchange control requirements.
2. All transactions made in a foreign currency on the Visa Card or wearable device will be converted into Australian currency by Visa Worldwide, and calculated at a wholesale market rate selected by Visa from within a range of wholesale rates or the government mandated rate that is in effect one day

prior to the Central Processing Date (that is, the date on which Visa processes the transaction).

3. All transactions made in a foreign currency on the Visa Card or wearable device are subject to a conversion fee. Please refer to the *Fees & Charges* brochure for the current conversion fee.
4. Some overseas merchants and electronic terminals charge a surcharge for making a transaction using your Visa Card or wearable device. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.
5. Some overseas merchants and electronic terminals allow the cardholder or wearable device user 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.
6. As Visa is an international payment facility, you may find that payment processing time-frames differ from one country to another. This is because different countries operate on different time zones, such as America who are one day behind Australia. All international card or wearable device based transactions are effective dated according to the date and time the transaction is conducted on the merchant terminal. This effective date will correspond with the date and time as shown on your transaction receipt received from the merchant. This means that when making deposits to your linked accounts to allow for Visa international purchases, you should ensure that you have enough funds available at least 2 days prior to making a purchase to avoid any dishonour fees that could result from differences in payment processing times.

Section 15. ADDITIONAL ACCESS CARD OR WEARABLE DEVICE

1. You may authorise us, if we agree, to issue:
   (a) an additional access card to an additional cardholder
   (b) a wearable device to an additional user

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

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

Section 16. USE AFTER CANCELLATION OR EXPIRY OF ACCESS CARD OR WEARABLE DEVICE

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

Section 17. EXCLUSIONS OF ACCESS CARD AND WEARABLE DEVICE WARRANTIES AND REPRESENTATIONS

1. We do not warrant that merchants or ATMs displaying access card or wearable device signs

or promotional material will accept access card or wearable device.

2. We do not accept any responsibility should a merchant, bank or other institution displaying access card or wearable device signs or promotional material, refuse to accept or honour access card or wearable device.

3. We are not responsible for any defects in the goods and services you acquire through the use of the Visa Card or wearable device. You acknowledge and accept that all complaints about these goods and services must be addressed to the supplier or merchant of those goods and services.

Section 18. CANCELLATION OF ACCESS CARD, WEARABLE DEVICE OR OF ACCESS TO HOME BANKING SERVICE, BPAY OR OSKO

1. You may cancel your access card, your wearable device, your access to telephone banking, internet banking, BPAY or Osko at any time by giving us written notice.
2. We may immediately cancel or suspend your access card, your wearable device or your access to telephone banking, internet banking , BPAY or Osko at any time:
   (a) for security reasons,
   (b) if you breach these Conditions of Use
   (c) you, or someone acting on your behalf, is being fraudulent
   (d) we suspect that you are using Osko in a manner that is likely to affect our ability to continue providing Osko to you or our other customers
   (e) if we cease to be a participant in Osko.
   (f) in the case of access card, we may cancel the access card bycapture of the access card at any ATM.
3. We may cancel your access card, your wearable device or your access to telephone banking, internet banking, BPAY or Osko for any reason by giving you 30 days notice. The notice does not have to specify the reasons for cancellation.
4. In the case of access card and wearable device, you will be liable for any transactions you make using your access card or wearable device before the access card or wearable device is cancelled but which are not posted to your account until after cancellation of access card or wearable device.
5. In the case of telephone banking, internet banking, BPAY or Osko, if, despite the cancellation of your access to telephone banking, internet banking, BPAY or Osko, you carry out a transaction using the relevant access method, you will remain liable for thattransaction.
6. Your access card, your wearable device or your access to telephone banking, internet banking, BPAY or Osko will be terminated when:
   (a) we notify you that we have cancelled your access card, your wearable device or your access method to the account with us;
   (b) you close the last of your accounts with us to which the access card or wearable device applies or which has telephone banking, internet banking, BPAY or Osko access;
   (c) you cease to be our member; or
   (d) you alter the authorities governing the use of your account or accounts to which the access card or wearable device applies or which has telephone banking, internet banking, BPAY or Osko access (unless we agree otherwise).
7. In the case of access card and wearable device, we may demand the return or destruction of any cancelled access card or wearable device.

Section 19. USING BPAY

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

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

Section 20. PROCESSING BPAY PAYMENTS

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

   Please keep a record of the BPAY receipt numbers on the relevant bills.
2. A BPAY payment instruction is irrevocable.
3. Except for future-dated payments you cannot stop a BPAY payment once you have instructed us to make it and we cannot reverse it.
4. We will treat your BPAY payment instruction as valid if, when you give it to us, you use the correct access method.
5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay.

   Please note that you must provide us with written consent addressed to the biller who received that BPAY payment. If you do not give us that consent, the biller may not be permitted under law to disclose to us the information we need to investigate or rectify that BPAY payment.
6. A BPAY payment is treated as received by the biller to whom it is directed:
   (a) on the date you direct us to make it, if we receive your direction by the cut off time on a banking business day, that is, a day in Sydney or Melbourne when banks can effect settlements through the Reserve Bank of Australia; and
   (b) otherwise, on the next banking business day after you direct us to make it.
   (c) Please note that the BPAY payment may take longer to be credited to a biller if you tell us to make it on a Saturday, Sunday or a public holiday or if another participant in BPAY does not process a BPAY payment as soon as they receive its details.
7. Notwithstanding this, a delay may occur processing a BPAY payment if:
   (a) there is a public or bank holiday on the day after you instruct us to make the BPAY payment;
   (b) you tell us to make a BPAY payment on a day which is not a banking business day or after the cut off time on a banking business day; or
   (c) a biller, or another financial institution participating in BPAY, does not comply with its BPAY obligations.
8. If we are advised that your payment cannot be processed by a biller, we will:
   (a) advise you of this;
   (b) credit your account with the amount of the BPAY payment; and
   (c) take all reasonable steps to assist you in making the BPAY payment as quickly as possible.
9. You must be careful to ensure you tell us the correct amount you wish to pay. If you make a BPAY payment and later discover that:
   (a) the amount you paid was greater than the amount you needed to pay - you must contact the biller to obtain a refund of the excess; or
   (b) the amount you paid was less than the amount you needed to pay - you can make another BPAY payment for the difference between the amount you actually paid and the amount you needed to pay.
10. If you are responsible for a mistaken BPAY payment and we cannot recover the amount from the person who received it within 20 banking business days of us attempting to do so, you will be liable for that payment.

Section 21. FUTURE-DATED BPAY PAYMENTS

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

1. You may arrange BPAY payments up to 365 days in advance of the time for payment. If you use this option you should be aware of the following:
   (a) you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all future-dated BPAY payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose.
   (b) if there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY payment will not be made and you may be charged a dishonour fee.
   (c) you are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly.
   (d) you should contact us if there are any problems with your future-dated payment.
   (e) you must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY payment on or after that date.

Section 22. CONSEQUENTIAL DAMAGE FOR BPAY PAYMENTS

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

Section 23. USING OSKO

1. You can use Osko® to make payments from those accounts that have the Osko facility.
   (a) make an Osko payment
   (b) make scheduled and recurring Osko payments
   (c) receive payment reminders
   (d) pay bills bearing the Osko logo from those accounts that have the Osko facility.
2. When you tell us to make an Osko payment you must tell us the payee's PayID or the details of the payee's account, the amount to be paid and the account from which the amount is to be paid.
3. We cannot effect your Osko instructions if you do not give us all the specified information or if you give us inaccurate information.

Section 24. PROCESSING OSKO PAYMENTS

1. We will attempt to make sure that your Osko payments are processed promptly by participants in Osko, and you must tell us promptly if:
   (a) you become aware of any delays or mistakes in processing your Osko payment;
   (b) you did not authorise an Osko payment that has been made from your account; or
   (c) you think that you have been fraudulently induced to make an Osko payment.
2. A Osko payment instruction is irrevocable.
3. Except for scheduled and recurring Osko payments, you cannot stop an Osko payment once you have instructed us to make it and we cannot reverse it.
4. We will treat your Osko payment instruction as valid if, when you give it to us, you use the correct access method.
5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay).
6. If we are advised that your payment cannot be processed by a biller, we will:

(a) advise you of this;

(b) credit your account with the amount of the Osko payment; and

(c) take all reasonable steps to assist you in making the Osko payment as quickly as possible.

Section 25. SCHEDULED AND RECURRING OSKO PAYMENTS

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

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

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

(b) if there are insufficient cleared funds or, as relevant, insufficient available credit, the Osko payment will not be made and you may be charged a dishonour fee;

(c) you are responsible for checking your account transaction details or account statement to ensure that the scheduled or recurrent Osko payment is made correctly;

(d) you should contact us if there are any problems with your scheduled or recurrent Osko payments;

(e) you must contact us if you wish to cancel a scheduled or recurrent Osko payment after you have given the direction but before the date for payment.

Section 26. AUTHORITY TO RECOVER MISTAKEN OR MISDIRECTED PAYMENTS

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

Section 27. REGULAR PAYMENT ARRANGEMENTS

1. You should maintain a record of any regular payment arrangement that you have entered into with a Merchant.
2. To change or cancel any regular payment arrangement you should contact the Merchant or us at least 15 days prior to the next scheduled payment. If possible you should retain a copy of this change/cancellation request.
3. Should your card details be changed (for example if your Visa Card was lost, stolen or expired and has been replaced) then you must request the Merchant to change the details of your existing regular payment arrangement to ensure payments under that arrangement continue. If you fail to do so your regular payment arrangement may not be honoured, or the Merchant may stop providing the goods and/or services.
4. Should your Visa Card or your accounts with us be closed for any reason, you should immediately contact the Merchant to change or cancel your regular payment arrangement, as the Merchant may stop providing the goods and/or services.

Section 28. APPLE PAY

When you add your Community First Visa Card onto your Apple device you are agreeing to these Conditions of Use.

Instructions on how to add your Visa Card to your Apple device, or remove it, and how to use Apple Pay on your device, are set out at on the following web pages:

- https://www.communityfirst.com.au/tools/apple-pay
- https://www.communityfirst.com.au/tools/apple-pay/faqs

Security of your Apple device

You must take reasonable steps to prevent unauthorised access to your Apple device. Anyone who accesses your Apple device could use it to make transactions on your Visa Card. You must ensure that:

- only your fingerprint, and no-one else's, is registered in your Apple device
- you do not allow anyone else's fingerprint to remain registered on your Apple device after you have loaded your Visa Card
- you keep your Apple device safe and secure
- you lock your Apple device when you are not using it or when you are leaving it unattended
- you install up-to-date anti-virus software on your Apple device
- you remove the Visa Card details from your Apple device before disposing of it.

If you allow another person's fingerprint to be registered on your Apple device, or you share the device's passcode, you will be taken to have authorised that person to carry out transactions from your Apple device.

WARNING: These transactions will be taken as yours and could lead to your incurring significant loss.

Steps you can take to protect your Apple device:

- **remove someone else's fingerprint registered to your Apple device**
- **change the pass code to access your Apple device**
- **delete or suspend your Visa Card from Apple Pay**

For the purposes of the ePayments section of our Credit Union Account and Access Facility:

- 'pass code' includes the pass code to your Apple Device
- the pass code security requirements that apply to the pass code of your Visa Card also apply to the pass code to your Apple device.

Apple Pay provided by Apple

Community First is not responsible for the functionality of the Visa Card on your Apple device other than supplying information to Apple to enable you to use the Visa Card on your Apple device. Apple is responsible for your Apple device's ability to communicate your Visa Card details at EFTPOS terminals.

ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE

Customer Owned banking delivers member-focused, competitive services. Credit unions, mutual banks and mutual building societies are customer-owned financial institutions committed to putting their members first.

The Customer Owned Banking Code of Practice, the code of practice for credit unions, mutual banks and mutual building societies, is an important public expression of the value we place on improving the financial wellbeing of our individual members and their communities.

Our 10 Key Promises to you are

1. We will be fair and ethical in our dealings with you
2. We will focus on our members
3. We will give you clear information about our products and services
4. We will be responsible lenders
5. We will deliver high customer service and standards
6. We will deal fairly with any complaints
7. We will recognise member rights as owners
8. We will comply with our legal and industry obligations
9. We will recognise our impact on the wider community
10. We will support and promote this Code of Practice.

You can download a copy of the Customer Owned Banking Code of Practice here
https://www.communityfirst.com.au/support/important-information/cobcop

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

Code Compliance Committee
PO Box 14240
Melbourne VIC 8001
Phone: 1300 367 287
Fax: 03 9613 7481
Email: info@codecompliance.org.au
www.cobccc.org.au/for-consumers/resolving-complaints/

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

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

You can contact the Australian Financial Complaints Authority:
by calling 1800 931 678
by visiting www.afca.org.au