



Account and Access Facility  
**Conditions of Use**

**First Option**  
Easy Banking  
designed for you

First Option Credit Union Limited  
ABN 95 087 650 735

## HOW TO CONTACT US

Visit one of our branches - for full branch details visit our website [www.firstoptioncu.com.au](http://www.firstoptioncu.com.au).

In Person                      Level 4, 409 St Kilda Road  
Melbourne Vic 3004

489 Harris Street  
Ultimo NSW 2007

1 Memorial Drive  
Granville NSW 2142

Phone us on                    1300 855 675

Write to us at                PO Box 7063  
St Kilda Road Vic 8004

Fax us on                      1800 356 675

Email us                        [info@firstoptioncu.com.au](mailto:info@firstoptioncu.com.au)

### **To report the loss, theft or unauthorised use of your VISA Card or Redicard:**

- In Australia

Call 1300 855 675, 24 hours a day, 7 days a week.

- Overseas

Call + 61 3 9869 8700, 24 hours a day, 7 days a week.

Visit the "Contact Us" page on our website for a list of Visa Global Assistance Hotlines for the country you are in.

If you report your card lost or stolen after hours, please contact First Option during business hours to order a replacement card.

To report the loss of any other access facility, or any type of unauthorised transaction, contact us as above.

## **CUSTOMER OWNED BANKING CODE OF PRACTICE**

We warrant that we will comply with the Customer Owned Banking Code of Practice. Please see the section 'About the Customer Owned Banking Code of Practice' at the end of these Conditions of Use for more detail.

## **ePAYMENTS CODE**

We warrant that we will comply with the ePayments Code and the Customer Owned Banking Code of Practice.

## **HOW OUR CONDITIONS OF USE BECOME BINDING ON YOU**

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

### Accessing Copies of the Conditions of Use

Please keep these Conditions of Use in a safe place so you can refer to them when needed. Alternatively, you can view and download our current Conditions of Use from our website at [www.firstoptioncu.com.au](http://www.firstoptioncu.com.au)

## **THE FINANCIAL CLAIMS SCHEME**

The Financial Claims Scheme ensures that depositors with credit unions, banks, and building societies will be guaranteed repayment of their funds in the extremely unlikely event that any banking institution fails. The Scheme includes a guarantee of \$250,000 per person per institution.

For further information about the Scheme:

- visit the Australian Prudential Regulation Authority's (APRA's) website at [www.apra.gov.au](http://www.apra.gov.au)
- call APRA's Hotline on 1300 13 10 60

## TABLE OF CONTENTS

ACCOUNT OPERATIONS .....	1
WHAT IS THE FIRST OPTION CREDIT UNION ACCOUNT AND ACCESS FACILITY? .....	1
HOW DO I OPEN AN ACCOUNT? .....	1
PROOF OF IDENTITY REQUIRED .....	2
WHAT ACCOUNTS CAN I OPEN? .....	2
WHAT FEES AND CHARGES ARE THERE? .....	3
WHAT INTEREST CAN I EARN ON MY ACCOUNT? .....	3
WHAT ARE THE TAXATION CONSEQUENCES? .....	3
DISCLOSING YOUR TAX FILE NUMBER (TFN) .....	4
JOINT ACCOUNTS .....	4
TRUST ACCOUNTS .....	5
THIRD PARTY ACCESS .....	5
MAKING DEPOSITS TO THE ACCOUNT .....	5
DEPOSITING CHEQUES .....	6
WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT .....	6
DEBITING TRANSACTIONS GENERALLY .....	7
OVER THE COUNTER WITHDRAWALS .....	7
WITHDRAWALS USING OUR CORPORATE CHEQUES .....	7
OVERDRAWING AN ACCOUNT .....	8
SWEEP FACILITY .....	8
ACCOUNT STATEMENTS .....	9
WHAT HAPPENS IF I CHANGE MY NAME OR ADDRESS? .....	9
DORMANT ACCOUNTS .....	9
ACCOUNT COMBINATION .....	9
CLOSING ACCOUNTS AND CANCELLING ACCESS FACILITIES .....	10
NOTIFYING CHANGES .....	10
HOW WE SEND NOTICES & STATEMENTS .....	12
COMPLAINTS .....	12
MEMBER CHEQUING .....	13

DIRECT DEBITS.....	13
PAYPAL .....	15
DIRECT CREDITS.....	15
ePAYMENT FACILITIES & ePAYMENT CONDITIONS OF USE.....	16
SECTION 1 - INFORMATION ABOUT OUR ePAYMENT FACILITIES .....	16
SECTION 2 - DEFINITIONS .....	19
SECTION 3 - TRANSACTIONS .....	21
SECTION 4 - WHEN YOU ARE NOT LIABLE FOR LOSS .....	22
SECTION 5 - WHEN YOU ARE LIABLE FOR LOSS .....	23
SECTION 6 - PASSCODE SECURITY REQUIREMENTS .....	26
SECTION 7 - LIABILITY FOR LOSS CAUSED BY SYSTEM OR EQUIPMENT MALFUNCTION .....	28
SECTION 8 - NETWORK ARRANGEMENTS .....	28
SECTION 9 - MISTAKEN INTERNET PAYMENTS .....	29
SECTION 10 - USING TELEPHONE, INTERNET AND MOBILE BANKING.....	33
SECTION 11 - HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR ACCESS CARD OR PASSCODE .....	33
SECTION 12 - HOW TO REPORT UNAUTHORISED USE OF TELEPHONE, INTERNET OR MOBILE BANKING .....	34
SECTION 13 - USING THE ACCESS CARD .....	34
SECTION 14 - USING VISA CARD OUTSIDE AUSTRALIA .....	35
SECTION 15 - ADDITIONAL ACCESS CARD .....	36
SECTION 16 - USE AFTER CANCELLATION OR EXPIRY OF ACCESS CARD.....	36
SECTION 17 - EXCLUSIONS OF ACCESS CARD WARRANTIES AND REPRESENTATIONS .....	37
SECTION 18 - CANCELLATION OF ACCESS CARD OR OF ACCESS TO TELEPHONE, INTERNET AND MOBILE BANKING OR BPAY® .....	37
SECTION 19 - USING BPAY® .....	38

SECTION 20 - PROCESSING BPAY® PAYMENTS .....	39
SECTION 21 - FUTURE-DATED BPAY® PAYMENTS .....	41
SECTION 22 - CONSEQUENTIAL DAMAGE FOR BPAY® PAYMENTS .....	42
SECTION 23 - REGULAR PAYMENT ARRANGEMENTS.....	42
ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE .....	44
CODE COMPLIANCE COMMITTEE .....	45

## ACCOUNT OPERATIONS

### WHAT IS THE FIRST OPTION CREDIT UNION ACCOUNT AND ACCESS FACILITY?

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

- Redicard
- VISA Card
- Member chequing
- BPAY® (registered to BPAY Pty Ltd ABN 69 079 137 518)
- Telephone, Internet and Mobile Banking
- EFTPOS and ATM access
- Direct credits
- Direct debits
- Periodical payments
- Bank@Post
- RediPOS

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

### HOW DO I OPEN AN ACCOUNT?

You will need to become a Member of the Credit Union before we can issue the First Option Credit Union Account and Access Facility to you.

To become a Member you need to:

- complete a Membership Application Form; and
- subscribe for a \$2 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 Photo Card (NSW only);
- 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 without you also giving us all the other names that you are commonly known by.

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

## **WHAT ACCOUNTS CAN I OPEN?**

When we issue you with the First Option Credit Union Account and Access Facility, you have access to the S1 Access Saver account. You can then activate other accounts as needed.



Please first check the *Summary of Accounts & Availability of Access Facilities* document for the different account types available, any special conditions for opening, and the features and benefits of each account type.

You may obtain a copy of the *Summary of Accounts & Availability of Access Facilities* document from [www.firstoptioncu.com.au](http://www.firstoptioncu.com.au) or by telephoning us on 1300 855 675.

## **WHAT FEES AND CHARGES ARE THERE?**

Please refer to the *Fees and Charges* Schedule for current fees and charges.

We may vary *fees and charges* from time to time.

We will debit your primary operating account for all applicable government taxes and charges.

You may obtain a copy of the *Fees and Charges* schedule from [www.firstoptioncu.com.au](http://www.firstoptioncu.com.au) or by telephoning us on 1300 855 675.

## **WHAT INTEREST CAN I EARN ON MY ACCOUNT?**

Our *Interest Rates* schedule provides information about our current deposit and savings interest rates. Our website also has information about our current deposit and savings interest rates.

We may vary deposit or savings interest rates from time to time on all deposit accounts except our term deposit accounts.

Our *Summary of Accounts & Availability of Access Facilities* document discloses how we calculate and credit interest to your account.

## **WHAT ARE THE TAXATION CONSEQUENCES?**

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

## **DISCLOSING YOUR TAX FILE NUMBER (TFN)**

When you apply for the First Option Credit Union Account and Access Facility we will ask you whether you want to disclose your Tax File Number (TFN) or exemption. If you disclose it we will note your TFN against any account you activate.

You do not have to disclose your TFN to us. If you do not, we will deduct withholding tax from interest paid on the account at the highest marginal rate.

For a joint account, each holder must quote their TFN and/or exemption, otherwise withholding tax applies to all interest earned on the joint account.

Businesses need only quote their ABN instead of a TFN.

## **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;
- joint and several liability - each joint holder is individually liable for the full amount owing on the joint account.

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'.

## **TRUST ACCOUNTS**

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

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

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

## **THIRD PARTY ACCESS**

You can authorise us, in writing, 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 accounts you have access to under the First Option 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 fully trust.**

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 First Option branches
- 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 Australia Post using Bank@Post
- by cash deposit at TAB Agencies (where available)
- by cash or cheque at branches of the National Australia Bank using an encoded pay-in book,

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

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. This can take up to 5 business days. However, you can ask us for a special clearance for which we may charge a fee. Please refer to our *Fees and Charges* Schedule for our current fee for special clearances.

Please note that cheques drawn on an overseas institution have longer clearance periods. These clearance times are subject to change without notice.

A fee may apply for a deposit of an overseas cheque. Please refer to the *Fees and Charges* Schedule for details.

## **WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT**

You can make withdrawals from the account:

- over the counter at our branches
- by direct debit
- by purchasing a corporate cheque drawn by First Option on your behalf
- by Member cheque, if your account is linked to a Member cheque book
- via telephone, internet or mobile banking

- via BPAY® to make a payment to a biller
- at Australia Post via Bank@Post if your account is linked to a VISA Card or Redicard
- at ATMs, if your account is linked to a VISA Card or Redicard
- via EFTPOS terminals, if your account is linked to a VISA Card or Redicard (note that merchants may impose restrictions on withdrawing cash)

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

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 at our absolute discretion.

## **OVER THE COUNTER WITHDRAWALS**

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

- the *Summary of Accounts & Availability of Access Facilities* document for any restrictions on withdrawals applying to certain accounts;
- the *Fees and Charges* Schedule.

## **WITHDRAWALS USING OUR CORPORATE CHEQUES**

This is a cheque the Credit Union draws payable to a payee you nominate. You can purchase a corporate cheque from us - see the *Fees and Charges* Schedule.

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.

## **OVERDRAWING AN ACCOUNT**

You must keep sufficient cleared funds in your account to cover your cheque, direct debit and EFT transactions or any other withdrawal by any means.

If you do not, we can dishonour the transaction and charge dishonour fees – see the *Fees and Charges* Schedule.

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

- interest at our current overdrawn rate, calculated on the daily closing balance, and/or
- a fee for each day (or part of a day) your account is overdrawn: see the *Fees and Charges* schedule.

‘Cleared funds’ means the proceeds of cheque deposits in your account (once the cheque is cleared), cash deposits and direct credits.

## **SWEEP FACILITY**

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

## **ACCOUNT STATEMENTS**

We will send you account Statements at least every 6 months. You can ask us for an account statement at any time. We may charge a fee for providing additional Statements or copies – see the *Fees and Charges Schedule*.

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

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 i for our contact details.

## **WHAT HAPPENS IF I CHANGE MY NAME OR ADDRESS?**

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

## **DORMANT ACCOUNTS**

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

Once your account becomes dormant, we may:

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

If your account remains dormant for 3 years, we have a legal obligation to remit balances exceeding \$500 to the Australian Securities and Investment Commission (ASIC) as unclaimed money.

## **ACCOUNT COMBINATION**

If you have more than one account with us, we may apply a deposit balance in any account to any other deposit account in the same name which is overdrawn.

On termination of your Membership, we may combine all your accounts (whether deposit or loan accounts) you have with us provided the accounts are all in the same name.

We will not combine accounts if to do so would breach the Code of Operation for Centrelink Direct Credit Payments.

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

## **CLOSING ACCOUNTS AND CANCELLING ACCESS FACILITIES**

You may close your First Option Credit Union Account and Access Facility at any time. However, you will have to surrender your access facilities such as your Member cheque book and any cards at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding cheques, EFT transactions and fees, if applicable.

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

We can:

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

## **NOTIFYING CHANGES**

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



<b>Type of change</b>	<b>Notice we must give</b>
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Reducing the number of fee-free transactions permitted on your account	20 days
Changing the minimum balance to which an account keeping fee applies	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited to your account	20 days
Changing interest rates	On the day of change
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.

## **HOW WE SEND NOTICES & STATEMENTS**

We may send you notices and Statements:

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

If you agree, we may, instead of sending you a notice or Statement, post notices or Statements to our website for you to retrieve. We will tell you when information is available for you to retrieve, either at the time or on setting up a facility that will have regular postings to the website.

You can change your nominated email address, or revert to receiving paper notices or Statements, at any time.

## **COMPLAINTS**

We have a dispute resolution process to deal with any complaints you may have in relation to the First Option 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 branch and tell them that you want to make a complaint. Our Team have a duty to deal with your complaint under our dispute resolution policy. Our Team 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 process available to you on request.

## **MEMBER CHEQUING**

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

If you have insufficient funds in your nominated account we may instruct the Bank to dishonour your cheque. However, we have the 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 or fees. Please refer to the section *Overdrawing An Account* on page 8.

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 years of age.

## **DIRECT DEBITS**

There are two types of Direct Debits, depending on your needs:

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

To cancel the DDR Service Agreement, you can contact either the biller or us. If you contact us we will promptly stop the facility. We suggest that you also contact the biller.

If you believe a direct debit initiated by a biller is wrong you should contact the biller to resolve the issue. Alternatively, you may contact us.

If you give us the information we require we will forward your claim to the biller. However, we are not liable to compensate you for your biller's error.

If you set up a payment on you VISA Card, please contact us directly about unauthorised or irregular debits.

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

2. The second type of Direct Debit (formerly known as a QuickDebit) is where you authorise First Option to debit funds from an account you hold at another financial institution and transfer them into your First Option account. You may apply to First Option to set up a Direct Debit by completing the Direct Debit Application form. Please refer to the *Direct Debit Request Service Agreement* for terms and conditions.

You must ensure that there are sufficient cleared funds available on the day the debit is due to allow the payment to be made. Should the payment fall on a non business day, the Direct Debit may be requested on the previous business day.

If there are insufficient cleared funds to cover a Direct Debit

- You may be charged a fee and/or interest by your financial institution
- You may be charged a fee and/or interest by us – refer to the *Fees and Charges* schedule, and
- You will need to arrange for the payment to be made by an alternative method

If you wish to defer a payment, change the arrangement, stop a payment, or cancel your direct debit request you must notify us in writing at least thirty (30) days before the next debit day. This notice should be given to us in the first instance.

We may cancel a Direct Debit facility at our absolute discretion.

## **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 you 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.

## **DIRECT CREDITS**

You may have your salary or any other regular payments credited to your account by Direct Credit. Approval is at the discretion of the Credit Union. Direct Credits may be allocated to any nominated account; nominated allocations must be in writing. We reserve the right to refuse to accept deposits from a Direct Credit Remitter.

The Direct Credit Remitter must provide sufficient funds to us to credit your Account and comply with any conditions that we imposed from time to time. Direct Credits received daily are to be processed as soon as possible. We are not liable for any delay in the crediting of your salary or other credit to your nominated Account.

We may reverse a Direct Credit to any of your accounts that the Credit Union has received on your behalf, if we for any reason whatsoever, do not receive value for the direct credit. To stop a Direct Credit payment service you must notify your Direct Credit Supplier and the Credit Union without delay after deciding to stop the service.

## **ePAYMENT FACILITIES & ePAYMENT CONDITIONS OF USE**

### **SECTION 1 - INFORMATION ABOUT OUR ePAYMENT FACILITIES**

You should follow the guidelines below to protect against unauthorised use of your devices and passcodes. A passcode is a number that only you know and should never be disclosed to another person.

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 your access card as soon as you receive it.
- Familiarise yourself with your obligations to keep your devices 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®, telephone, internet or mobile banking.
- If you change a passcode, do not select a code or password which represents your birth date or a recognisable part of your name.
- Never write the PIN passcode on your access card.
- Never write the PIN passcode on anything which is kept with or near your access card.
- Never lend your access card to anybody.

- Never tell or show your passcodes to another person.
- Use care to prevent anyone seeing your 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 telephone, internet or mobile banking services 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 any of your passcodes. We will NEVER ask you to provide us with these details.

**If you fail to ensure the security of your access card, access facility and password 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:

Redicard	Visa Card
BPAY®	Internet Banking
Mobile Banking	Telephone Banking

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

## **Redicard**

Redicard allows you to access your account via Bank@Post at Australia Post outlets and any ATM or EFTPOS terminal in Australia displaying the Redicard logo. We will provide you with a PIN to use with your Redicard.

Redicard allows you to:

- withdraw cash from your account; and
- deposit cash or cheques into your account (using Bank@Post at Australia Post only).

We may choose not to give you a Redicard if you are under 16 years of age.

## **VISA Card**

VISA Card allows you to make purchases at any retailer displaying the VISA logo, anywhere in the world. You can also withdraw cash from your account, anywhere in the world, using an ATM displaying the VISA logo. We will provide you with a PIN to use with your VISA Card. A VISA Card also allows you to:

- withdraw cash from your account;
- deposit cash or cheques into your account (using Bank@Post at Australia Post only);
- pay your bills from billers who accept VISA; and
- purchase goods and services online by using the VISA facility.

We may choose not to give you a VISA Card if your banking history with the Credit Union is not satisfactory, or if you are under 18 years of age.

## **Important Information about Chargebacks for VISA Card**

If you believe a VISA Card transaction was:

- unauthorised;
- 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. However, we can only do a chargeback if you inform us of the disputed transaction within the timeframe determined by VISA. Currently the shortest cut-off time for notifying of chargeback circumstances is 45 days after the transaction, although longer periods may apply in particular circumstances.

You are not able to reverse a transaction authenticated using Verified by VISA 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 copy of the Visa transaction receipt in question.**

## **SECTION 2 - DEFINITIONS**

- (a) **access card** means an ATM card, debit card or credit card and includes our VISA Card and Redicard
- (b) **ATM** means automatic teller machine
- (c) **business day** means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned
- (d) **device** means a device we give to a user that is used to perform a transaction. Examples include:
  - (i) ATM card
  - (ii) debit card or credit card
  - (iii) token issued by a subscriber that generates a passcode
- (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) **passcode** means a password or code that the user must keep secret, that may be required to authenticate a transaction or user. A passcode may consist of numbers, letters, a combination of both, or a phrase. Examples include:
- (i) personal identification number (PIN)
  - (ii) internet banking NetCode
  - (iii) telephone banking access code
  - (iv) code generated by a security token or SMS.

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

- (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 ePayment Conditions of Use apply
- (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 First Option Credit Union
- (o) **you** means the person or persons in whose name this Account and Access Facility is held

### **SECTION 3 - TRANSACTIONS**

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

## **SECTION 4 - WHEN YOU ARE NOT LIABLE FOR LOSS**

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 passcode which is forged, faulty, expired or cancelled
  - (c) a transaction requiring the use of a device and/or passcode that occurred before the user received the device and/or password (including a reissued device and/or passcode)
  - (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 passcode has been breached.
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 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 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

- (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.

## **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 passcode 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 passcode 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 passcode used to perform the transaction.
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 Section 6 or one or more of the required passcodes, but not all of the required passcodes then you are liable under clause 5.2 only if we also prove

on the balance of probability that the breach of the passcode 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 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
  - (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 5.5 if you were the user who contributed to the loss, or if a different user contributed to the loss.*

6. Where a passcode 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 passcode, including any prearranged credit
  - (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 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 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 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, chargeback 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 - PASSCODE SECURITY REQUIREMENTS**

1. Section 6 applies where one or more passcodes are needed to perform a transaction.
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
    - (ii) liable to loss or theft simultaneously with a deviceunless the user makes a reasonable attempt to protect the security of the passcode
  - (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).
3. For the purpose of clauses 6.2(b) - 6.2(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
- (d) preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

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, 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 passcode by a user, see clause 6.5.*

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
  - (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 passcode 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 passcode that is required or recommended for the purpose of using the service does not breach the passcode 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 as described below.
7. When we receive a complaint 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**

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

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

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

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

**Process where funds are available & report is made between 10 business days & 7 months**

- The receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request.
- If satisfied that a mistaken internet payment has occurred, the receiving ADI must:
  - a. prevent the unintended recipient from withdrawing the funds for 10 further business days, and
  - b. notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds.
- If the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after

the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their account.

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

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

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

### **Process where funds are not available**

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

## **SECTION 10 - USING TELEPHONE, INTERNET AND MOBILE BANKING**

1. We do not warrant that:
  - (a) the information available to you about your accounts through our phone 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, internet or mobile banking is totally secure.

## **SECTION 11 - HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR ACCESS CARD OR PASSCODE**

1. If you believe your access card has been misused, lost or stolen or the passcode 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 i 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 hotline is available 24 hours a day, 7 days a week.
4. If the 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 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:
  - (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 (refer to How to Contact Us on page i).

## **SECTION 12 - HOW TO REPORT UNAUTHORISED USE OF TELEPHONE, INTERNET OR MOBILE BANKING**

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

*Please refer to How to Contact Us on page i 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 passcode, you should change that passcode.

## **SECTION 13 - USING THE ACCESS CARD**

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 to time:
  - (a) what transactions may be performed using an access card;



- (b) what ATMs of other financial institutions may be used; and
- (c) what the daily cash withdrawal limits are.

*Please refer to the Fees and Charges Schedule and Summary of Accounts and Availability of Access Facilities document for details of current transaction limits*

- 3. You may only use your access card to perform transactions on those accounts we permit. We will advise you of the accounts which you may use your access card to access.
- 4. The access card always remains our property.

## **SECTION 14 - USING VISA CARD OUTSIDE AUSTRALIA**

- 1. You agree to reimburse us for any costs, fees or charges of any nature arising out of a failure to comply with any exchange control requirements.
- 2. All transactions made overseas on the Visa Card will be converted into Australian currency by Visa Worldwide, and calculated at a wholesale market rate selected by Visa from within a range of wholesale rates or the government mandated rate that is in effect one day prior to the Central Processing Date (that is, the date on which Visa processes the transaction).
- 3. All transactions made overseas on the Visa Card are subject to a conversion fee payable to CUSCAL, the principal member of Visa Worldwide under which First Option can provide you with the Visa card. Please refer to the *Fees and Charges Schedule* for the current conversion fee.
- 4. Some overseas merchants and ATMs charge a surcharge for making a transaction using your Visa card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.

## **SECTION 15 - ADDITIONAL ACCESS CARD**

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

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

## **SECTION 16 - USE AFTER CANCELLATION OR EXPIRY OF ACCESS CARD**

1. You must not use your access card:
  - (a) before you authorise First Option to activate the card or after the expiration date shown on the face of the access card; or

(b) after the access card has been cancelled.

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

## **SECTION 17 - EXCLUSIONS OF ACCESS CARD WARRANTIES AND REPRESENTATIONS**

1. We do not warrant that merchants or ATMs displaying access card signs or promotional material will accept your access card.
2. We do not accept any responsibility should a merchant, bank or other institution displaying access card signs or promotional material, refuse to accept or honour your access card.
3. We are not responsible for any defects in the goods and services you acquire through the use of the Visa Card. You acknowledge and accept that all complaints about these goods and services must be addressed to the supplier or merchant of those goods and services.

## **SECTION 18 - CANCELLATION OF ACCESS CARD OR OF ACCESS TO TELEPHONE, INTERNET AND MOBILE BANKING OR BPAY®**

1. You may cancel your access card, your access to telephone, internet and mobile banking or BPAY® at any time by contacting First Option.
2. We may immediately cancel or suspend your access card or your access to telephone, internet and mobile banking or BPAY® at any time for security reasons or if you breach these Conditions of Use. In the case of an access card, we may cancel the access card by capture of the access card at any ATM.
3. We may cancel your access card or your access to telephone, internet and mobile banking or BPAY® 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 an access card, you will be liable for any transactions you make using your access card before the access card is cancelled but which are not posted to your account until after cancellation of access card.
5. In the case of telephone, internet and mobile banking or BPAY<sup>®</sup>, if, despite the cancellation of your access to telephone, internet and mobile banking or BPAY<sup>®</sup>, you carry out a transaction using the relevant access method, you will remain liable for that transaction.
6. Your access card or your access to telephone, internet and mobile banking or BPAY<sup>®</sup> will be terminated when:
  - (a) we notify you that we have cancelled your access card or your access method to the account with us;
  - (b) you close the last of your accounts with us to which the access card applies or which has telephone, internet and mobile banking or BPAY<sup>®</sup> 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 applies or which has telephone, internet and mobile banking or BPAY<sup>®</sup> access (unless we agree otherwise).
7. In the case of an access card, we may demand the return or destruction of any cancelled access card.

## **SECTION 19 - USING BPAY<sup>®</sup>**

1. You can use BPAY<sup>®</sup> to pay bills bearing the BPAY<sup>®</sup> logo from those accounts that have the BPAY<sup>®</sup> facility.
2. When you tell us to make a BPAY<sup>®</sup> payment you must tell us the biller 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 action your BPAY<sup>®</sup> 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<sup>®</sup> PAYMENTS**

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

*Please keep a record of the BPAY<sup>®</sup> receipt numbers on the relevant bills.*

2. A BPAY<sup>®</sup> payment instruction is irrevocable.
3. Except for future-dated payments you cannot stop a BPAY<sup>®</sup> payment once you have instructed us to make it and we cannot reverse it.
4. We will treat your BPAY<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> payment.*

6. A BPAY<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> does not process a BPAY<sup>®</sup> payment as soon as they receive its details.
7. Notwithstanding this, a delay may occur processing a BPAY<sup>®</sup> payment if:
  - (a) there is a public or bank holiday on the day after you instruct us to make the BPAY<sup>®</sup> payment;
  - (b) you tell us to make a BPAY<sup>®</sup> 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<sup>®</sup>, does not comply with its BPAY<sup>®</sup> 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<sup>®</sup> payment; and
  - (c) take all reasonable steps to assist you in making the BPAY<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> PAYMENTS**

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

You may arrange BPAY<sup>®</sup> payments up to 60 days in advance of the time for payment. If you use this option you should be aware of the following:

- (a) You are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all future-dated BPAY<sup>®</sup> 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<sup>®</sup> 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 - 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.

## **ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE**

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

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

*Our 10 Key Promises to you are:*

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

You can download a copy of the Customer Owned Banking Code of Practice from the Customer Owned Banking Association website:

<http://www.customerownedbanking.asn.au>

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 78 08 08  
Fax: 03 9613 7481  
info@codecompliance.org.au  
www.cccmutuals.org.au

The Code Compliance Committee 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 Financial Ombudsman Service, directly. However, they will refer the complaint back to us to see if we can resolve it directly with you before involving them.

You can contact the Financial Ombudsman Service:

by calling 1300 78 08 08  
by visiting <http://www.fos.org.au>

This page has  
intentionally been left blank