SOUTH WEST SLOPES CREDIT UNION ACCOUNT & ACCESS FACILITY

Conditions of Use

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

Date taking effect: August 2016

The South West Slopes Credit Union Account and Access Facility is issued by:
South West Slopes Credit Union Ltd.
ACN 087 650 673
ABN 80 087 650 673
AFS & Australia Credit Licence No. 240712

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

Please keep the Conditions of Use brochure in a safe place so you can refer to it or visit www.swscu.com.au to view.

HOW TO CONTACT US

Visit us at any of our branches or visit our website at www.swscu.com.au for our branch details

Head Office, South West Slopes Credit Union Ltd, PO Box 84, Young, NSW, 2594

Telephone: 02 6384 1111 Facsimile: 02 6382 1744

To report the loss, theft or unauthorised use of your VISA card:

Telephone: 02 6384 1111, After hours 24 Hour Lost or Stolen Card Hotline 1800 648 027

VISA Card Overseas

If the loss, theft or misuse occurs OUTSIDE AUSTRALIA you must notify a Financial Institution displaying the VISA logo and you must also then confirm the loss, theft or misuse of the card with us by telephone or priority paid mail as soon as possible

Please contact us prior to travelling to obtain up to date contact information relevant to your destination country. Alternatively for international callers phone the 24hr Emergency Hot Line on +61 2 82999101 (not toll free).

Refer to the *VISA Card Conditions of Use document Section 5* for further information on your obligations if your VISA is lost, stolen or misused outside of Australia.

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 Electronic Funds Transfer Code of Conduct and any other relevant industry code of practice that may apply.

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

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

PRIVACY

We have a Privacy Statement that sets out:

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

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

HOW OUR CONDITIONS OF USE BECOME BINDING ON YOU

Please note 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 the Conditions of Use brochure in a safe place so you can refer to when needed. Alternatively, you can view and download our current Conditions of Use from our website at www.swscu.com.au

THE 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 SOUTH WEST SLOPES CREDIT UNION ACCOUNT AND ACCESS FACILITY?

The South West Slopes 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 - Debit and/or Credit
- Member Chequing
- BPAY® (registered to BPay Pty Ltd ABN 69 079 137 518) - limits apply
- BPayView
- EPAY – limits apply
- Telephone and Internet banking
- EFTPOS and ATM access
- Direct Debit requests
- Direct Credit requests
- Bill Paying

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

HOW DO I OPEN A MEMBERSHIP?

To become a member, you will need to:

- complete a membership application form; and
- subscribe for a member share in the Credit Union (at a cost to you of $10.00 for one share)

The member share is a redeemable preference share. This means that, when you resign your membership with the Credit Union, we refund you the subscription price ($10.00). Please note that your member share is not transferable.

You must subscribe for membership in the same name as the account you wish to open. However, you can open an account jointly with another person, so long as you are both members of the Credit Union. Each member requires a $10.00 share for membership.

Provide Proof of Identity

The law requires us to verify your identity when you open an account or when you become a signatory to an 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;
- 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 South West Slopes Credit Union Account and Access Facility, you have access to an "S1" account. This is your primary operating account with the Credit Union, and you can then activate other accounts as needed. Please refer to the *Summary of Accounts & Availability of Access Facilities* brochure for the different account types available, any special conditions for opening, and the features and benefits of each account type.

WHAT ARE THE FEES AND CHARGES?

Please refer to the *Fees & Charges and Transaction Limits* brochure for our current fees and charges. We may vary fees or charges from time to time. Please see Changing Fees, Charges, Interest Rates and Other Information for details of how and when we must notify you of these changes.

WHAT INTEREST CAN I EARN ON MY ACCOUNT?

We calculate and credit interest to your account as set out in the *Summary of Accounts & Availability of Access Facilities* 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 interest rates from us at any time or by visiting our website at www.swscu.com.au .

WHAT ARE THE TAXATION CONSEQUENCES?

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

When you apply for the South West Slopes Credit Union Account and Access Facility we will ask you whether you want to disclose your Tax File Number 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 joint memberships, each holders must quote their Tax File Numbers and/or exemptions; otherwise withholding tax applies to all interest earned on the joint account.

Businesses need only quote their ABN instead of a TFN..

JOINT MEMBERSHIPS

A joint membership is in the name of more than one person. The important legal consequences of holding a joint membership 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 – each joint holder is individually liable for the full amount owing on the joint membership.

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 accountholder 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 MEMBERSHIPS

You can open a membership as a trust. However:

- we are not aware of the terms of the trust; or
- we do not have to verify that any transactions you carry out on the membership 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 membership. However, we will need to verify this person's identity before they can access your membership.

You can specify which of your accounts under the South West Slopes Credit Union Account & Access Facility you give the authorised person authority to operate on. 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 branch
- by direct credit
- by transfer from another account with us
- by transfer from another financial institution
- by cash or cheque at a National Australia Bank branch using a specially encoded deposit book

Note that electronic deposits may not be processed on the same day. Please refer to EFT Conditions of Use:

DEPOSITING CHEQUES

You can only access the proceeds of a cheque when it has cleared. This usually takes four (4) business days. However, you can ask us for a special clearance for which we may charge a fee. Please refer to our *Fees & Charges and Transaction Limits* brochure for our current fee for special clearances.

WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT

You can make withdrawals from the account:

- over the counter at South West Slopes Credit Union branch or agency
- by direct debit
- by member cheque, if your account is linked to this facility
- via telephone or internet banking
- via BPAY® to make a payment to a biller
- via EPAY to transfer funds to another institution within Australia
- 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 (please note that merchants may impose restrictions on withdrawing cash)
- via Bill Pay

DEBITING TRANSACTIONS GENERALLY

We will debit transactions received on any one day in the order we determine in our absolute discretion.

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 a Credit Union corporate cheque. Please refer to:

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

If a corporate cheque is lost or stolen, you can ask us to stop payment. To process this request our Indemnity form must be completed.

We cannot stop payment on our corporate cheque if the cheque was used 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 require assistance.

OVERDRAWING AN ACCOUNT

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

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

- interest at our current overdraft rate, calculated on the daily closing balance; and
- a referral fee refer to the *Fees & Charges and Transaction Limits* brochure.

'Cleared funds' means cash deposits, direct credits or the proceeds of cheque deposit(s) to your account, once the cheques have cleared.

SWEEP FACILITY

You may nominate an 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.

MEMBER STATEMENTS

We will send member statements at least every six (6) months. You can request an interim statement on any account at any time. We may charge a fee for providing additional member statements or copies refer to the *Fees & Charges and Transaction Limits* brochure.

We recommend that you check your member statement as soon as you receive it and immediately notify us of any unauthorised transactions or errors. Please refer to *How to Contact Us.*

WHAT HAPPENS IF I CHANGE MY NAME?

We recommend that if you change your name, you let us know immediately.

WHAT HAPPENS IF I CHANGE MY CONTACT DETAILS?

Please notify us via telephone if you would like to change your address, telephone number, fax number or email address.

DORMANT MEMBERSHIPS

If no transactions are carried out on your membership for at least twelve (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 Seven (7) years, we have a legal obligation to remit balances exceeding $500.00 to the Australian Securities and Investment Commission as unclaimed money. For children's accounts, unclaimed money will be remitted to ASIC after 7 years.

MEMBERSHIP COMBINATION

If you have more than one membership with us, we may apply a deposit balance to any other membership in the same name which is overdrawn. We may also transfer funds between accounts within a membership to adjust overdrawn accounts.

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 do so if this 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.

CHANGING FEES, CHARGES, INTEREST RATES AND OTHER INFORMATION

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

Type of change	Notice we must give	Manner of giving notice
a.. increasing any fee or charge	20 days	in writing
b. adding a new fee or charge	20 days	in writing
c. reducing the number of fee-free transactions permitted on your account	20 days	in writing
d. changing the method by which interest is calculated	20 days	in writing
e. changing the circumstances when interest is credited to your account	20 days	in writing
f. changing any other term or condition	When we next communicate with you	As applicable

CLOSING MEMBERSHIPS AND CANCELLING ACCOUNT AND ACCESS FACILITIES

When you close your membership with South West Slopes Credit Union the Account and Access Facility is cancelled. We will require the return of any unused cheques and any access card before the membership can be closed. 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. However, for direct debits, you must contact the third party to cancel any direct debit authority;

We can:

- close your membership with South West Slopes Credit Union and cancel the Account and Access Facility in our absolute discretion by giving you reasonable notices and paying you the balance of your membership; or
- cancel any access facility for security reasons or if you breach these Conditions of Use.

NOTICES & 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.

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.

You can vary your nominated email address at any time or cancel arrangements to receive notices by email.

COMPLAINTS

We have a dispute resolution system to deal with any complaints you may have in relation to The South West Slopes Credit Union Account and Access Facility or transactions on the account. Our dispute resolution policy requires us to deal with any complaint efficiently, quickly and sympathetically. If you are not satisfied with the way in which we resolve your complaint, or if, we do not respond within one business day, you may refer the complaint to the Financial Ombudsman Service.

If you want to make a complaint, contact our staff at any branch and tell them that you want to make a complaint. Our staff members 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. 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 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 and fees. Please refer to the section Overdrawing An Account.

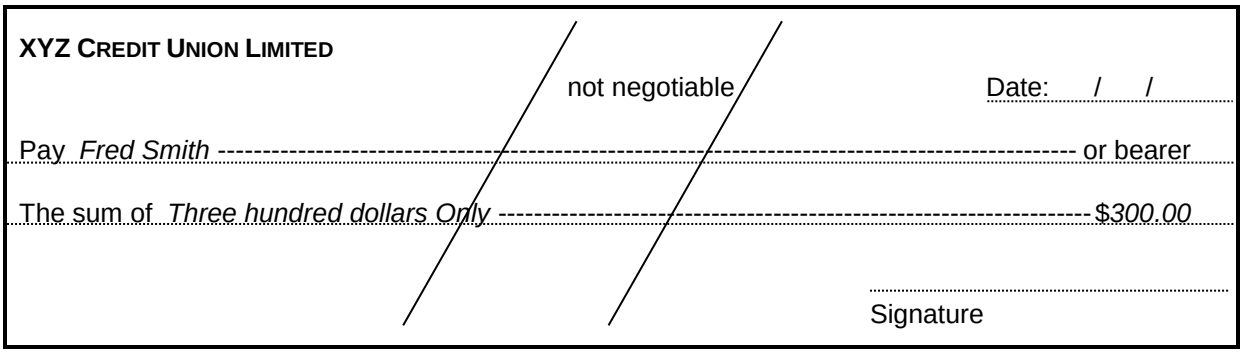
We may not give you access to member chequing if your banking history with the Credit Union is not satisfactory, or if you are under eighteen (18) years of age.

CHEQUE SECURITY

Crossing a cheque, 'not negotiable' or 'account payee only'

If you cross a cheque, it is a direction to us to pay the cheque into an account at a bank or other financial institution. A crossing does not actually prevent the cheque being negotiated or transferred to a third party before presentation to a bank or financial institution for payment.

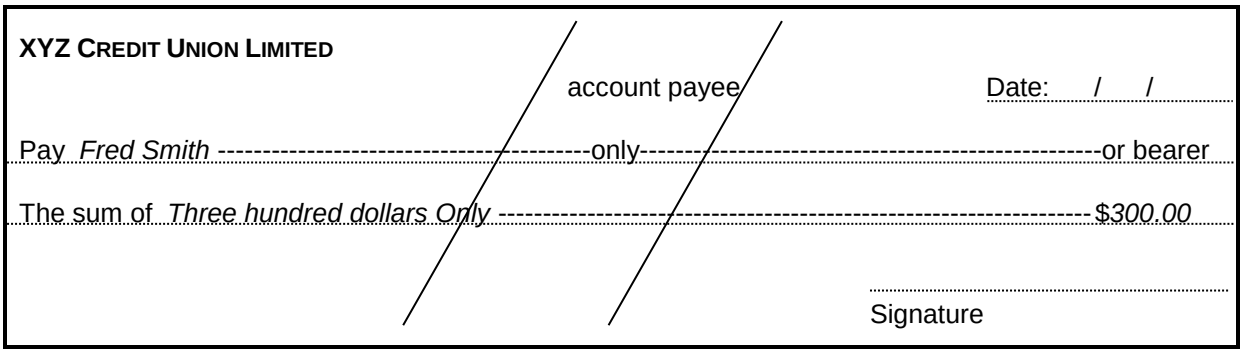
Example of 'not negotiable' crossing:



Crossing a cheque means drawing 2 lines clearly across the face of the cheque as shown above.

When you cross a cheque or add the words 'not negotiable' between the crossing you may be able to protect yourself, but not always, against theft or fraud. This crossing sometimes serves as a warning to the collecting financial institution, if there are other special circumstances, that it should enquire if its customer has good title to the cheque.

Example of 'account payee' crossing:



When you add the words 'account payee only' between these lines you are saying that only the named person can collect the proceeds of the cheque. These words may give you better protection against theft or fraud. It would be prudent for the collecting financial institution to make enquiries of the customer paying the cheque in, if the customer is not the payee of the cheque.

Deleting 'or bearer' on the cheque

Your pre-printed cheque forms have the words 'or bearer' after the space where you write the name of the person to whom you are paying the cheque. The cheque is a 'bearer' cheque. If you cross out the words 'or bearer' and do not add the words 'or order', the cheque is still a bearer cheque. You can give yourself more protection against theft or fraud by crossing out the words 'or bearer' and adding the words 'or order'.

How do I stop payment on a cheque?

You can stop payment on a cheque by:

- ringing us with sufficient particulars to identify the cheque; we may insist on written confirmation; or
- writing to us, again, with sufficient particulars to identify the cheque.

You must, of course, do this before we paid the cheque.

What do I do to reduce the risk of forgery?

When filling in a cheque:

- start the name of the person to whom you are paying the cheque as close as possible to the word 'Pay';
- draw a line from the end of the person's name to the beginning of the printed words 'or bearer';
- start the amount in words with a capital letter as close as possible to the words 'The sum of' and do not leave blank spaces large enough for any other words to be inserted; also add the word 'only' after the amount in words;
- draw a line from the end of the amount in words to the printed '$';
- start the amount in numbers close after the printed '$' and avoid any spaces between the numbers;
- always add a stop '.' or dash '–' to show where the dollars end and the cents begin and, if there are no cents, always write '.00' or '–00' to prevent insertion of more numbers to the dollar figure.

Example:

XYZ CREDIT UNION LIMITED

Date: / /

Pay *Fred Smith* ----------or bearer

The sum of *Three hundred dollars Only* ----------$*300.00*

Signature

When can we dishonour or not pay your cheque?

We can dishonour your cheque if:

- you have insufficient funds or available credit in your account to cover the cheque;
- you have not drawn up the cheque clearly so we are unsure what you want to do;
- you have post-dated your cheque and it is presented for payment before the date on the cheque;
- the cheque is 'stale', that is, the date of the cheque is more than twelve (12) months ago; or
- we have notice of your death or mental incapacity.

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 may provide you with a Direct Debit Request (DDR) Service Agreement for you to complete and sign.

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.

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

BILL PAYING

You can also provide us with instructions to make periodical payments from your account. You must give us at least one (1) business days' notice in writing to stop any periodical payment you have instructed us to make.

We can cancel your bill pay authority in our absolute discretion, if five (5) consecutive attempts are declined.

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 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 and pass codes secure.
- Familiarise yourself with the steps you have to take to report loss or theft of your access card or to report unauthorised use of your access card, BPAY® or telephone or internet banking.
- Immediately report lost, theft or unauthorised use.
- 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.
- Never write the pass code PIN on anything which is kept with or near the access card.
- Never lend the access card to anybody.
- Never tell or show the pass code to another person.
- Use care to prevent anyone seeing the pass code being entered on 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, access facility and pass codes you may increase your liability for unauthorised transaction.

THESE EPAYMENT CONDITIONS OF USE GOVERN ALL ELECTRONIC TRANSACTIONS MADE USING ANY ONE OF OUR ELECTRONIC ACCESS FACILITIES, LISTED BELOW:

Visa Card	Internet Banking
BPAY®	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*

Visa Card

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

- check your account balances;
- withdraw cash from your account;

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 (Visa Classic Credit Card only).

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. You can do so by telling us within 30 days after the date of the statement which shows the transaction and providing us with any information we may require. 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.

Telephone and Internet Banking

Telephone and internet banking gives you remote access to your account that allows you to obtain information about your account, to transfer money between accounts, to make BPAY® payments and to transfer money to accounts at other financial institutions, using a pass code.

BPAY®

BPAY® allows you to pay bills bearing the BPAY® logo, through either telephone or internet banking.

SECTION 2: DEFINITIONS

(a) **Access card** means an ATM card, debit card or credit card and includes our Visa Debit and Visa Credit Cards.

(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 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 a person 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, and

(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).

(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, 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 South West Slopes Credit Union Ltd

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

Section 3. TRANSACTIONS

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

(a) initiated using electronic equipment, and

(b) not intended to be authenticated by comparing a manual signature with a specimen signature.

3.2 These ePayment Conditions of Use apply to the following transactions:

(a) electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature

(b) telephone banking and bill payment transactions

(c) internet banking transactions, including 'Pay Anyone'

(d) online transactions performed using a card number and expiry date

(e) online bill payments (including BPAY)

(f) direct debits

(g) transactions using mobile devices.

Section 4. PASS CODE SECURITY REQUIREMENTS

4.1 This section applies where one or more pass codes are needed to perform a transaction.

4.2 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).

4.3 For the purpose of clauses 4.2(b)–4.2(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.

4.4 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 4.5.

4.5 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.

4.6 The onus is on us to prove, on the balance of probability, that we have complied with clause 4.5.

4.7 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 this Section.

4.8 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 4.

Section 5. HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR VISA CARD OR PASS CODE

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

Please refer to How to Contact Us for our contact details.

5.2 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.

5.3 The Visa Card HOTLINE is available 24 hours a day, 7 days a week.

5.4 If the Visa 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 Visa 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.

Section 6. HOW TO REPORT UNAUTHORISED USE OF TELEPHONE OR INTERNET BANKING

6.1 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 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.

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

Section 7. USING VISA CARD

7.1 You agree to sign the Visa Card immediately upon receiving it and before using it as a means of preventing fraudulent or unauthorised use of the Visa Card. You must ensure that any other cardholder you authorise also signs their Visa Card or immediately upon receiving it and before using it.

7.2 We will advise you from time to time:

(a) what transactions may be performed using the Visa 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 & Charges and Transaction Limits* brochure *for details of current transaction limits Also note that we can vary daily withdrawal limits from time to time.*

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

7.4 The Visa Card always remains our property.

Section 8. USING VISA OUTSIDE AUSTRALIA

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

8.2 All transactions made in a foreign currency on the Visa Card are subject to a conversion fee. . Please refer to the *Fees & Charges and Transaction Limits* brochure for the current conversion fee.

8.3 Some overseas merchants and electronic terminals charge a surcharge for making a transaction using your Visa card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.

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

Section 9. ADDITIONAL VISA CARD

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

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

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

9.4 You must ensure that any additional cardholders protect their Visa Card and pass code in the same way as these EFT Conditions of Use require you to protect your Visa Card and pass code.

9.5 To cancel the additional Visa Card you must notify us in writing. However, this cancellation may not be effective until the additional Visa Card is returned to us or you have taken all reasonable steps to have the additional Visa Card returned to us.

9.6 You will not be liable for the continued use of the additional Visa 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 Visa Card returned to us.

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

Section 10. USE AFTER CANCELLATION OR EXPIRY OF THE VISA CARD

10.1 You must not use your Visa Card:

(a) before the valid date or after the expiration date shown on the face of the Visa Card ; or

(b) after the Visa Card has been cancelled.

10.2 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 11. EXCLUSIONS OF VISA CARD WARRANTIES AND REPRESENTATIONS

11.1 We do not warrant that merchants or ATMs displaying Visa Card signs or promotional material will accept the Visa Card.

11.2 We do not accept any responsibility should a merchant, bank or other institution displaying Visa Card signs or promotional material, refuse to accept or honour the Visa.

11.3 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 12. CANCELLATION OF VISA CARD OR OF ACCESS TO HOME BANKING SERVICE OR BPAY

12.1 You may cancel your Visa Card, your access to telephone banking, internet banking or BPAY at any time by giving us written notice.

12.2 We may immediately cancel or suspend your Visa Card or your access to telephone banking, internet banking or BPAY at any time for security reasons or if you breach these EFT Conditions of Use. In the case of Visa Card, we may cancel the Visa Card by capture of the Visa Card at any ATM.

12.3 We may cancel your Visa Card or your access to telephone banking, internet banking or BPAY for any reason by giving you 30 days notice. The notice does not have to specify the reasons for cancellation.

12.4 In the case of Visa Card or, you will be liable for any transactions you make using your Visa Card before the Visa Card is cancelled but which are not posted to your account until after cancellation of the Visa Card.

12.5 In the case of telephone banking, internet banking or BPAY, if, despite the cancellation of your access to telephone banking, internet banking or BPAY, you carry out a transaction using the relevant access method, you will remain liable for that transaction.

12.6 Your Visa Card or your access to telephone banking, internet banking or BPAY will be terminated when:

(a) we notify you that we have cancelled your Visa Card or your access method to the account with us;

(b) you close the last of your accounts with us to which the Visa Card applies or which has telephone banking, internet banking or BPAY 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 Visa Card or applies or which has telephone banking, internet banking or BPAY access (unless we agree otherwise).

12.7 In the case of Visa Card, we may demand the return or destruction of any cancelled Visa Card.

Section 13. USING BPAY

13.1 You can use BPAY® to pay bills bearing the BPAY logo from those accounts that have the BPAY facility.

13.2 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.

13.3 We cannot effect your BPAY instructions if you do not give us all the specified information or if you give us inaccurate information.

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

Section 14. PROCESSING BPAY PAYMENTS

14.1 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.

14.2 A BPAY payment instruction is irrevocable.

14.3 Except for future-dated payments you cannot stop a BPAY payment once you have instructed us to make it and we cannot reverse it.

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

14.5 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 - for these errors see section 14.9) when making a BPAY payment or if you did not authorise a BPAY payment that has been made from your account.

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.

14.6 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.

14.7 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.

14.8 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.

14.9 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.

14.10 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 15. FUTURE-DATED BPAY PAYMENTS

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

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

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

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

(c) You are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly.

(d) You should contact us if there are any problems with your future-dated payment.

(e) You must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY payment on or after that date.

Section 16. CONSEQUENTIAL DAMAGE FOR BPAY PAYMENTS

16.1 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.

16.2 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 17. REGULAR PAYMENT ARRANGEMENTS

17.1 You should maintain a record of any regular payment arrangement that you have entered into with a Merchant.

17.2 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.

17.3 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.

17.4 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 18. WHEN YOU ARE NOT LIABLE FOR LOSS

18.1 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.

18.2 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.

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

18.4 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 19. WHEN YOU ARE LIABLE FOR LOSS

19.1 If Section 18 does not apply, you may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this Section 4.

19.2 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 4:

(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.

19.3 Where:

(a) more than one pass code is required to perform a transaction

(b) we prove that a user breached the pass code security requirements in Section 4 for one or more of the required pass codes, but not all of the required pass codes

you are liable under clause 19.2 only if we also prove on the balance of probability that the breach of the pass code security requirements under Section 4 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

19.4 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.

19.5 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 19.5 if you were the user who contributed to the loss, or if a different user contributed to the loss.

19.6 Where a pass code was required to perform an unauthorised transaction, and clauses 19.2-to 19.5 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.

19.7 In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under clauses 19.2 to 19.5:

(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 4

(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.

19.8 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 4 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 20. LIABILITY FOR LOSS CAUSED BY SYSTEM OR EQUIPMENT MALFUNCTION

20.1 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.

20.2 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 21. NETWORK ARRANGEMENTS

21.1 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.

21.2 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 22. MISTAKEN INTERNET PAYMENTS

22.1 In this Section 22:

(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

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

22.3 If satisfied that a mistaken internet payment has occurred, 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.

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

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

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

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

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

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

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

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

22.5 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.

22.6 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

(i) have not complied with the processes and timeframes set out in clauses 22.2 to 22.5.

22.7 When we receive a complaint under clause 22.6 we must:

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

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

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

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.

HOW TO CLAIM A 'PAY ANYONE' AMOUNT

On our member's instructions we will send you an SMS or email telling you how much our member, the payer, wants to pay into your bank account and giving you a collection code. To claim the payment you must follow the instructions in the SMS or email and provide the following information:

- your mobile phone number or email address, corresponding to the mobile or email address to which we sent our SMS
- the exact amount of the payment you are claiming
- the collection code
- details of the account to which you wish the payment to be made

WARNING

WE ARE NOT ABLE TO CARRY OUT A MATCH OF THE BSB, ACCOUNT NUMBER AND YOUR NAME TO ENSURE THAT THE DETAILS YOU HAVE GIVEN US ARE CORRECT.

FOR THIS REASON YOU MUST TAKE EXTREME CARE TO ENSURE THAT ALL OF THE DETAILS YOU GIVE US – BSB AND ACCOUNT NUMBER – ARE CORRECT.

IF YOU ENTER ANY OF THIS INFORMATION INCORRECTLY PLEASE RING US AS SOON AS YOU CAN. WE ARE NOT ABLE TO REVERSE THE TRANSACTION ONCE WE HAVE SENT IT BUT MAY BE ABLE TO PUT IN PLACE PROCEDURES TO RECOVER THE PAYMENT FOR OUR MEMBER. YOU WILL THEN NEED TO CONTACT OUR MEMBER TO ARRANGE FOR A REPLACEMENT PAYMENT TO BE MADE WHICH WILL ONLY OCCUR ONCE OUR MEMBER HAS RETRIEVED THE MONEY FROM THE UNINTENDED ACCOUNT YOU SENT IT TO.

You have 14 days after receipt of our SMS or email to nominate your account. Technically, the cut off time is midnight AEST on the 14th day following notification by SMS or email. Also, it can take up to 3 days for the payment to be processed into your account.

Please be aware that our member can instruct us to cancel the payment at any time prior to your nominating your account details. Also, we may cancel the payment instruction at any time for technical reasons.

PRIVACY INFORMATION

When you utilise this service we will be collecting your personal information in order to provide the service. We will be sharing that information with other parties in the Australian Financial Settlement System. Your bank account details are kept securely and only disclosed within the Australian

Financial Payment System or to regulators and enforcement authorities in exercise of statutory rights to collect information and data.

PAY ANYONE CONDITIONS OF USE

When you use the collection code to claim a payment you will be entering into a contract with our member (the payer) and us as follows:

1. We, South West Slopes Credit Union Ltd act as the payer's agent and not your agent.
2. You agree to use the collection code for the purpose it was given to you, that is, to nominate your account details to us so we can complete the payment instructions on the payer's behalf.
3. You agree not to divulge the collection code except for the purpose we have been instructed to give it to you.
4. Once we make a payment to an account you nominate by use of the collection code you agree that the payment discharges the payer's liability to pay you regardless of who owns the account you have nominated.
5. We may cancel the collection code at any time before the collection code is used to authorise a payment to an account.
6. Once you use the collection code to nominate the account to which we are to send the payment you are unable to cancel or vary the nomination because we will have already acted on your nomination and sent the payment.
7. **It is your responsibility to ensure that the account you nominate, and the account details you provide, using the collection code, are correct**.
8. You agree that we, South West Slopes Credit Union Ltd, and the member are not liable to you for making the payment to an account you nominate, even if you make a mistake in the account details.

ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE

Customer Owned banking delivers member-focused, competitive services. Credit unions 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 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

http://www.customerownedbanking.asn.au/consumers/cobcop

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

Code Compliance Committee Mutuals
PO Box 14240
Melbourne VIC 8001
Phone: 1300 78 08 08
Fax: 03 9613 7481
info@codecompliance.org.au
www.cccmutuals.org.au/resolving-complaints/how-the-ccc-can-help/

The Code Compliance Committee Mutuals (Consumer Credit Code) 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 1800 367 287
by visiting http://www.fos.org.au

SCHEDULE OF REVIEW AND AMENDMENTS

Date	Action
30 October 2008	Updated (VISA)
28 October 2009	Re-Issued (DB Legal June 2009) Various Updates
7 January 2010	VISA Card - Regular Payment Arrangements, Bill Paying
28 June 2010	Updated (VISA) clauses to ensure covered for Debit Card
27 June 2012	Epayments Codes, Direct Debits, Financial Claims Scheme and About the MBCOP sections amended.
28 August 2012	Re-Issued (DB Legal 27/08/12) amending some elements of 12/06/12 update
30 January 2013	All rediCARD references removed
30 April 2013	Inserted new section “How to Claim ‘Pay Anyone” Amount – Mobile App
13 March 2014	Changed MBCOP to COBCOP; Dormant Membership from seven (7) to three (3) years, Reviewed due to privacy compliance and unclaimed monies regulation.
3 August 2016	Changed reference to FGS and APRA