Terms and Conditions for Internet & Mobile Banking

About these terms and conditions

These terms and conditions contain important information about using Summerland Credit Union's Internet Banking service on your computer or mobile device. You must read and accept these terms and conditions before using Internet Banking. You should also refer to our General Terms and Conditions which contains information about our products and services, and our Schedule of Fees and Charges, which lists all the fees and charges you may incur when using our products and services.

We subscribe to the ePayments Code. You can find a copy of the Code on the Australian Securities and Investments Commission website.

Getting started

To use Internet Banking, you will need your customer number and a passcode. When you first sign up for Internet Banking, we will give you a temporary passcode to log in for the first time. You will be prompted to set your own passcode when you log in.

Your passcode

Your passcode is a combination of uppercase and lowercase letters, numbers and symbols. You can change your passcode anytime in Internet Banking.

Make sure you create a passcode that nobody else will be able to guess. Do not use your date of birth, telephone number, any other easily-guessed series of characters or your name. The strongest passcodes include at least one uppercase and lowercase letter, a number and a symbol.

You must keep your passcode secret. Do not share it with anyone including family, friends and other institutions, or let anyone else see it. Never write your passcode down without making reasonable attempts to keep it safe. Never store your passcode with your computer or internet-enabled device.

We will never ask you for your passcode.

Unauthorised use of your passcode should be reported to us immediately. If you suspect that someone else has used your passcode, knows your passcode, or you have written your passcode down and lost it, you should tell us and change it as soon as possible.

Call 1300 802 222 and talk to one of our banking advisors during business hours. You can also visit our website for more information.

Internet and computer security

In addition to keeping your passcode safe, there are some other things you can do to stay secure when using Internet Banking.

Make sure your computer or internet-enabled device is free from malware by keeping your software up-to-date. Use reputable and reliable antivirus and firewall software.

Do not open email attachments if they look suspicious or you were not expecting to receive them. Do not give anyone your personal information or passcode when asked in an email. We will never ask for your passcode and, if we ask you for personal information, we will call you first.

Always remember to log out of Internet Banking when you are finished.

You are responsible for the security and maintenance of your computer or internet-enabled device. We are not liable for any damage or loss you suffer as a result of a malfunction of your computer or internet-enabled device, or because of a disruption to your internet connection.

Two-factor authentication is the most secure way of logging in to Internet Banking. When two-factor authentication is enabled, you will need your customer number, passcode, and a randomly generated code sent to your phone or token. For more information, please speak to us.

Electronic communication

If you use Internet Banking, we will send you important information by electronic communication. You agree to the provision of notices and statements to you through internet Banking.

You will no longer receive paper notices or statements, unless we cannot give you the notice or statement electronically.

We will send emails to the email address you nominate. You must ensure your nominated email address is up-to-date.

Making payments

We will accept your payment instructions when you log in securely to Internet Banking and give us all the information we need to effect the transaction. You are responsible for the accuracy of the information you give us, such as BSB and account numbers.

If you ask us to make a payment, but close the account to be debited before we process that payment, you will still have to pay any related fees. We can refuse to make a payment and we are not liable for any loss or damage you or another person suffer because the payment was not made.

You should keep any receipt numbers we give you.

BPay® payments cannot be cancelled unless they are future-dated. Other organisations like billers and financial institutions may impose restrictions on how you use BPay®.

Future-dated payments can be a one-off payment, or a series of regular payments, made up to 90 days in advance of the selected due date. A payment won't be made unless there are sufficient funds in the relevant account to cover the payment by midnight on the previous day.

If there are not enough funds to meet a one-off future-dated payment, the payment will not occur. If you are making a series of regular payments, we will continue to make those as long as there are sufficient funds in the account by midnight of the day before the next payment.

You can cancel future-dated payments using Internet Banking. You can also speak to us and we will cancel it. We cannot cancel future-dated payments that have already occurred.

A **Mistaken payment** is a payment by a user through a ‘Pay Anyone’ internet or mobile banking 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 BSB and/or identifier that does not belong to the named and/or intended recipient as a result of:

- the user's error, or
- the user being advised of the wrong BSB number and/or identifier.

This excludes payments made using BPAY, incorrect transactions such as duplications or incorrect amounts or disputed or unauthorised transactions.

You must take care to enter or select the correct information about the intended recipient of the funds, required when using Pay Anyone to make a payment. It is not always possible for us to recover funds from the unintended recipient. If the receiving ADI is unable to recover the funds from the unintended recipient you will be liable for losses arising from the mistaken internet payment. You should report a mistaken internet payment to us as soon as possible.

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

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

- acknowledge the request by the sending ADI for the return of funds, and
- advise the sending ADI whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

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.

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

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

- are not satisfied that a mistaken internet payment has occurred; or
- have not complied with the required processes and timeframes.

When we receive a complaint we must deal with the complaint under our internal dispute resolution procedures and not require you to complain to the receiving ADI.
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.

If you receive a mistaken internet payment into your account we as the receiving ADI may be required to act in accordance with the ePayments Code.

The table below 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.

You can report a mistaken payment to us at any time, but the process that will apply to seek the return of funds will depend upon when the report of the mistaken internet transaction was made.

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:
  1. prevent the unintended recipient from withdrawing the funds for 10 further business days, and
  2. 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:
  1. the receiving ADI must return the funds to the sending ADI, and
  2. 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).

Liability for payments

Your liability for payments made through Internet Banking is governed by the ePayments Code.

You are not liable for loss arising from an unauthorised payment where the payment was caused by

- fraud or negligence by any of our employees or agents;
- a forged, faulty, expired or cancelled device, identifier or passcode;
- use of a device or passcode that you had not yet received at the time the payment was made;
- a transaction being incorrectly debited more than once to the same account; or

- an unauthorised transaction performed after you had told us that a device or passcode had been misused, lost, stolen or compromised.

You are also not liable where it is clear that you have not contributed to the loss arising from an unauthorised transaction.

You are liable where
- you, or someone else with your consent, instructed us to make a payment;
- you contributed to the loss through fraud or breaching the above guidelines on passcode security; or
- you unreasonably delayed reporting the misuse, loss or theft of a device or passcode.

If you breached the above guidelines on passcode security, you will only be liable if your breach was more than 50 percent responsible for the loss. If you unreasonably delayed reporting the misuse, loss or theft of a device or passcode, your liability is limited to the portion of any loss
- incurred on any one day that is within your daily transaction limit;
- that is within the balance of the account, including any pre-arranged credit; and
- incurred between when you became, or should have become, aware of the misuse, loss or theft and the time you reported it to us.

In any other case, where a passcode was required to perform an unauthorised transaction, you will be liable for the least of
- $150.00;
- the balance of the account(s), including pre-arranged credit, that can be accessed using the passcode; or
- the actual loss at the time that the misuse, loss or theft of a device or passcode is reported to us, excluding the portion of the loss incurred on any one day that exceeds any daily transaction limit.

Service disruptions

You are not liable for any loss you incur because BPay® accepted your payment instructions but failed to make the payment. If there is a disruption to the BPay® service that you should have been aware of, we will only be responsible for correcting any errors in your account and refunding any fees or charges you incurred on your account due to the disruption.

We will do our best to make sure Internet Banking is always available for you. However, sometimes the service may be disrupted because of a malfunction or update. We are not liable to you for any loss you incur because of
- the failure of Internet Banking to perform any function;
- the failure of your internet connection, computer, internet-enabled device or other equipment beyond our control; and
- delays or errors in the making of a payment.

Your privacy

Your privacy is important to us. You should understand how we collect, use and disclose your personal information. Refer to our privacy notification and privacy policy for more information at http://www.summerland.com.au/why/creditunion/general?slide=1-2#your-privacy.

Cancelling your access to Internet Banking

If you do not log in to Internet Banking for a period of 90 days, your access will be cancelled to protect you and your accounts. To re-enable Internet Banking, simply speak to us.

Your access to Internet Banking will be suspended for 24 hours if you input the incorrect passcode three times in a row. If your access has been suspended and you have not attempted to log in

three times, someone else may be trying to access your account. Contact us immediately if you suspect that this has occurred.

We will cancel your access to Internet Banking when
- you cease to be a member;
- you close all of your accounts with us;
- you breach these terms and conditions; or
- we believe the security of your accounts has been compromised.

You can cancel your access to Internet Banking at any time by giving us written instructions.

Contacting us

Phone	1300 802 222 (overseas +612 6620 7098)
Mail	PO Box 657 LISMORE NSW 2480
Email	info@summerland.com.au
Fax	(02) 6622 6433
Website	summerland.com.au
Internet Banking	summerland.com.au/ib
Phone Banking	1300 221 999
SMS	0448 221 999