Terms and Conditions for Internet & Mobile Banking

About these terms and conditions

These terms and conditions contain important information about using Summerland Bank's Internet Banking service on your computer, smartphone, or internet-enabled device. Read these terms and conditions before using Internet Banking. By using Internet Banking, you become bound by these terms and conditions. Read our *Account and Access Facilities Conditions of Use* for information about our products and services including conditions of use of Osko and PayID. Read *Fees Charges and Transaction Limits* for fees and charges you may incur when using our products and services.

We subscribe to the Customer Owned Banking Code of Practice and the ePayments Code. More information about the Customer Owned Banking Code of Practice is in the *Account and Access Facilities Conditions of Use* on our website. You can find a copy of the ePayments Code on the Australian Securities and Investments Commission website.

Getting started

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

Your passcode

Your passcode combines 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. For example, do not use your date of birth, telephone number, your name or any other easily guessed series of characters. The strongest passcodes include at least one uppercase and lowercase letter, a number, and a symbol.

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, smartphone, or internet-enabled device.

We will **NEVER** ask you for your passcode.

Unauthorised use of your passcode should be reported to us immediately. If your passcode is lost or stolen or 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 immediately.

Call 1300 728 728 and talk to one of our banking advisors during business hours. You can also visit our website for more information.

Internet 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, smartphone 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 did not expect 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. Any such call will be during business hours, and we will identify ourselves. If in any doubt that you are speaking with us, hang up and call us on 1300 728 728.

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

You are responsible for the security and maintenance of your computer, smartphone, or internet-enabled device. We are not liable for any damage or loss you suffer due to:

- you permitting a third party to use your computer, smartphone, or internet-enabled device,
- a malfunction of your computer, smartphone, or internet-enabled device,
- if the smartphone used to access your online services is Jailbroken (iPhone) / Rooted (Android), or
- due to a disruption to your internet connection.

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

Electronic communication

If you use Internet Banking, you agree to receive important information through electronic communication and notices and statements through Internet Banking. Notifications of account activity will be sent to your email address confirming changes such as the adding of a new recipient to your address book or that your internet banking passcode or contact details have been updated, as well as an unsuccessful login attempt, changes to daily limits and failure of a scheduled transfer/BPay.

We will send emails to the email address you nominate. Therefore, 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 necessary information to effect the transaction. You are responsible for the accuracy of the payment instructions, such as BSB and account numbers. You should confirm the BSB and account numbers you have entered are correct. Payments are processed using these details without checking the account name. If the BSB or account number is incorrect, funds may be credited to the account of an unintended recipient. It may not be possible to recover funds from an unintended recipient.

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 suffered 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 may impose restrictions on how you use BPAY.

Future-dated payments can be a one-off payment or a series of regular payments, set up to 60 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 day before the due date.

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 if 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 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 BSB and/or identifier that does not belong to the named and/or intended recipient because of:

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

This does not include 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 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 take no 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 our resolution of your complaint, you can contact the Australian Financial Complaints Authority (AFCA), a free and impartial external dispute resolution scheme.

If we are unable to return funds to you because the unintended recipient of a mistaken internet payment does not cooperate, you can contact the Australian Financial Complaints Authority (AFCA).
If you receive a mistaken internet payment into your account, as the receiving ADI, we are obligated to act in a way consistent with the ePayments Code including where necessary reverse internet deposits mistakenly made to your account.

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 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:
  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).

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 when 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 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:
1. $150.00;
2. the balance of the account(s), including pre-arranged credit, that can be accessed using the passcode; or
3. 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 www.summerland.com.au/general-assistance.

Cancelling your access to Internet Banking

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 this has occurred.

We will cancel your access to Internet Banking when:

- you cease to be a member;
- you close all 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 728 728 (overseas +612 6620 7098)**
Mail	**PO Box 657** **LISMORE NSW 2480**
Email	**info@summerland.com.au**
Website	**summerland.com.au**
Internet Banking	**ib.summerland.com.au**
Phone Banking	**1300 221 999**
SMS	**0448 221 999**

® Registered to BPAY Pty Ltd ABN 69 079 137 518

Summerland Bank is a business name of Summerland Financial Services Limited

ABN 23 087 650 806
ASFL 239 238
Australian Credit Licence 239 238