

Security Information

If your card is lost or stolen or your PIN or Phone or Internet Banking access code is revealed

If your card is lost or stolen, you must notify us as soon as possible. You should also notify us if you suspect that someone else knows your PIN or you suspect any unauthorised use of your card by calling **1800 224 004**.

You should notify us if you suspect that someone else knows your Phone or Internet Banking access code or you suspect any unauthorised use of Phone or Internet Banking to operate your Sutherland Credit Union account by calling **1300 784 388** and you should immediately change your Phone access code by calling **(02) 9545 0588** or Internet access code via the Internet Banking website **www.sutherlandcu.com.au**

Liability for unauthorised transactions

This information is to assist you to look after the security of your card, PIN, Phone or Internet Banking access code. It does not state the circumstances in which either you or Sutherland Credit Union may be responsible for unauthorised transaction on your Sutherland Credit Union account(s).

Sutherland Credit Union is guided by the liability provisions of the Electronic Funds Transfer Code of Conduct to determine responsibility for unauthorised electronic transactions on your Sutherland Credit Union account(s).

Contact Details

Lost & Stolen Cards (24 Hours): **1800 224 004**

RediPhone Banking: **(02) 9545 0588**

Website: **www.sutherlandcu.com.au**

Email: **memberlink@sutherlandcu.com.au**

MemberLink (9am–5pm, Mon- Fri): **1300 784 388**



Sutherland Credit Union Limited
ABN 89 087 650 708 AFSL 238070

Security Information Guide



SUTHERLAND
credit union

Security Information

How to protect your access methods

To help ensure the security of your electronic banking access methods, we ask you to:

- Immediately sign your card as soon as you receive it.
- Avoid using public computers for Internet Banking, eg: Internet cafes, libraries or hotels.
- Check that any telephone system you use does not record your Phone or Internet Banking access code eg: some hotels or motels may record all numbers entered.
- Take reasonable steps to protect the security of your computer's hardware and software.
- Keep your computer anti-virus and firewall software up-to-date.
- Make sure that nobody watches you enter your PIN, Phone or Internet Banking access code.
- You should also look out for suspicious devices placed on or near ATMs or key pads.
- Ensure your PIN is not recorded on your card or any item that could be lost or stolen with your card.
- Make sure your Phone or Internet Banking access code is not written on the computer or telephone that you use to access Phone or Internet Banking.
- Ensure your Phone or Internet Banking access code is not recorded on any item that identifies your Phone and Internet Banking access number (i.e. Member number) or on any article that could be lost or stolen with that item.
- Do not permit any other person to use your card or your Phone or Internet Banking access code.
- Ensure you do not disclose your PIN, Phone or Internet Banking access code, or make it available to any other person (including family members, friends or our staff).

Selecting your own PIN, Phone and Internet Banking access code

You can select your own PIN at any Sutherland Credit Union branch and your own Phone or Internet Banking access code when you first use Phone or Internet Banking.

When you select a PIN, Phone or Internet Banking access code you should select a code that you can remember without the need to make a written record of it.

Do not choose a number or a word that others might be able to guess (for example your date of birth, telephone numbers or an alphabetical code that is a recognisable part of your name or simple sequence of numbers like 1234).

If you select a PIN, it must comprise of four digits.

If you select a Phone access code, it must comprise 4, 5 or 6 digits. If you select a Internet banking access code it must comprise 4 - 8 digits and contain at least 1 number and 1 letter (A-Z , a-z) but not spaces. We recommend you select a Phone or Internet Banking access code that is different to any of your PINs.

We recommend you change you Phone and Internet Banking access codes regularly.

Recording a memory aid for your PIN, Phone and Internet Banking access code

If you require a memory aid to recall your PIN, Phone or Internet Banking access code, you may make a record of it, if you reasonable disguise the PIN or access code.

There may be some forms of disguising a PIN, Phone or Internet Banking access code that are unsuitable because they enable another person to work out your PIN, Phone or Internet Banking access codes easily. So, please do NOT:

- Record your PIN on your card
- Record your disguised Phone or Internet Banking access code on any item that identifies your Phone or Internet Banking access number (ie. Member number).
- Disguise your PIN, Phone or Internet Banking access code by reversing the numbers.
- Record your disguised Phone or Internet Banking access code on the computer or telephone that you use to access Phone and Internet Banking.
- Describe your disguised record as a "Phone or Internet Banking access code", "PIN record", "Internet Password" or similar.
- Disguise your PIN, Phone or Internet Banking access code using alphabetical characters or numbers such as A=1, B=2, C=3 etc.
- Store your PIN, Phone or Internet Banking access code in any low security electronic device of any kind, for example, calculators, personal computers or electronic organisers.