

# Access Method Security

To guard against unauthorised electronic transactions on your account, whether via the use of access cards, such as VISA or Redicards and a PIN, or through telephone and Internet banking services where an access code is used, we strongly suggest that you read and follow these security guidelines:

- Sign your access card as soon as you receive it
- Keep your cards in a safe place
- If you change the PIN or access code you must NOT select a PIN or code that represents your birth date or a recognisable part of your name
- Never write the PIN on the access card or place an access code on the telephone or your computer terminal
- Never write the PIN or access code on anything that is kept with or near your access cards, telephone or computer terminal
- Never lend your access cards to anybody
- Never tell or show your PIN or access codes to another person
- Use care to prevent anyone seeing the access card number and PIN being entered at Electronic Equipment (\*electronic equipment includes, amongst other things, a computer, telephone, television and an EFT terminal)
- Immediately report the loss, theft or unauthorised use of your access card to your credit union or other relevant body (such as the VISA CARD HOTLINE)
- Keep a record of the access card number and the contact telephone number for your area with your usual list of emergency telephone numbers
- After accessing secure areas for Internet banking it is suggested that you close your Internet browser after logging out

- Never leave your computer unattended while logged into your banking facilities.
- Never respond to e-mails requesting you to provide your internet banking member number and access code, even if the e-mail appears to be legitimate. Legitimate financial institutions will never ask for your information in this manner.
- Examine your periodical statement immediately upon receiving it to identify and report, as soon as possible, any instances where electronic transactions have occurred without your authority
- Immediately notify the credit union of any change of address.

Further information about security is available from the Australian Securities and Investments Commission (ASIC) website ([www.asic.gov.au](http://www.asic.gov.au)) in their publication "Consumer Alert - 10 tips for safer electronic banking and protecting yourself under the EFT Code". Following the guidelines does not mean that you cannot be liable for unauthorised transactions. Depending on the circumstances, you could be held liable for unauthorised transactions. For example, if you unreasonably delay advising the credit union after you become aware of the unauthorised transactions, or if you have contributed to the loss by your actions. The guidelines will NOT determine your liability for losses resulting from unauthorised transactions. Liability for such transactions is determined in accordance with the Conditions of Use applying to your access card, telephone or Internet services and the provisions of the EFT Code of Conduct. Information about the EFT Code of Conduct can be obtained from the Credit Union or ASIC's publication "Guide to the EFT Code" ([www.asic.gov.au](http://www.asic.gov.au)).

If you have any questions regarding the above mentioned information, please do not hesitate to contact New England Credit Union on 132067.