For general enquiries, contact the ANZ Customer Service Centre on **13 13 14**, 24 hours, 7 days. Hearing and speech impaired customers can utilise the TTY service: 1300 366 255. Alternatively, you may wish to contact us via our website, anz.com.

anz.com

ANZ Electronic Banking Security Guidelines

BUSINESS ACCOUNTS (EXCLUDING BUSINESS CREDIT CARDS) | 04.10

Guidelines for your Security Device, card and password security

Your ANZ card, Security Device, passwords, PIN, Telecode, Security Device Code (being the number generated by a Security Device or a substitute number provided by ANZ) and other usernames or passwords ("card, device and security passwords"), are the keys to accessing your accounts electronically. The security of your card, device and security passwords is therefore very important.

These guidelines are designed to help you keep your card, device and security passwords secure. By following these Guidelines, you can assist in preventing misuse of your ANZ card, device and security passwords.

Liability for unauthorised transactions will be determined under the ANZ Electronic Banking Conditions of Use (contained in your ANZ Product Disclosure Statement or product terms and conditions) and not under these guidelines.

Card Security

To help protect your card, you must:

- Sign the back of your card immediately on receipt;
- Not let anyone else use your card;
- Regularly check that you still have your card;
- Take reasonable steps to protect your card from loss or theft;
- Ensure that you retrieve your card after making a transaction;
- Notify ANZ immediately if you become aware that your card has been lost or stolen, or has been used by someone else; and
- Destroy your card on the expiry date by cutting it diagonally in half (including any embedded microchip on the card, magnetic strip and security code).

Security Device security

To help protect your Security Device, you must:

- Not let anyone else use your Security Device;
- Regularly check that you still have your Security Device;
- Take reasonable steps to protect your Security Device from loss or theft;
- Notify ANZ immediately if you become aware that your Security Device has been lost or stolen, or has been used by someone else;
- Not keep your Security Device near or with your password (even if your password is disguised); and
- Return your Security Device to ANZ at the address specified in the Electronic Banking Conditions of Use on the expiry date (printed on the back of the Security Device).

Password, PIN, Telecode and Security Device Code security

To help protect your password, PIN, Telecode and Security Device Code ("security passwords"), you must:

- Not disclose your security passwords to anyone including a family member or friend (you may, however, disclose your ANZ Phone Banking Password to an ANZ officer);
- Not enter your security passwords into a web page which has been accessed by a link from an email, even if the email may appear to have been sent by ANZ. When accessing ANZ Internet Banking you should always enter anz.com into your browser using the keyboard of your computer;
- Take care to prevent anyone else seeing your security passwords being entered in electronic equipment or hearing you disclose your Phone Banking Password (Security Code) to an ANZ officer;
- Not write or indicate your security passwords on your card or your Customer Registration Number(s) (CRN(s)) on your Security Device, even if they are disguised;
- Try to commit your security passwords (excluding Security Device Codes) to memory and not write or indicate your security passwords anywhere without reasonably disguising it;
- Notify ANZ immediately if you become aware that your security passwords records have been lost or stolen, or known or used by someone else;
- Not choose a password, PIN or Telecode which has an easily retrieved combination (for example, repeated numbers or letters); and
- Not choose a password, PIN or Telecode that is easily identified with you (for example, your birth date, car registration, telephone number or your name or part of it, including in reverse order).

What is NOT a reasonable attempt to disguise a password, PIN or Telecode

If you record your password, PIN or Telecode, you must make a reasonable attempt to disguise it. The following are examples of what is NOT a reasonable attempt to disguise your password, PIN or Telecode:

- Recording the password, PIN or Telecode in reverse order;
- Recording the password, PIN or Telecode as a telephone number where no other numbers are recorded;
- Recording the password, PIN or Telecode as a telephone number with the Password, PIN or Telecode in its correct sequence;
- Recording the password, PIN or Telecode among other numbers or letters with any of them marked to indicate the password, PIN or Telecode;
- Recording the password, PIN or Telecode disguised as a date (including your birth date) or as an amount; or
- Recording the password, PIN or Telecode in an easily understood code.

You must not use any other form of disguise that may be easily discovered by another person.