Protect your PIN and Card

- Sign your Cashcard or Visa card immediately when you receive it
- Always check any ATM or Eftpos machine you use for evidence of tampering – very discreet skimming devices can record your card number
- Always cover your PIN when at an ATM
- Keep your card and PIN separate at all times
- Do not record your PIN on, or with your card
- Do not disclose your PIN to anyone
- Do not allow anyone else to use your PIN or card
- Do not let anyone else see your PIN
- Register your Hume Visa card for Verified by Visa

Call us on 1300 004 863 to report unauthorised use, loss or theft.

Emergency After Hours:
Lost or stolen Cashcard, Visa cards or PINs
Phone 1800 252 730 – after hours

Liability for unauthorised transactions will be determined under the EFT Code of Conduct and not under these guidelines. However, failure by you to keep your card and code/PIN secure may increase your liability for unauthorised use.

Hume's Electronic Transaction Terms and Conditions that apply to the use of your card and PIN, internet banking and information on Hume's products are available in the Product Disclosure Statement (PDS) at any Hume branch or at **www.humebank.com.au**

Always report any unauthorised or suspicious transactions to us on **1300 004 863**.

Hume Bank limited. ABN 85 051 868 556 AFSL No. 244248

Hume Bank

Security Advice

Electronic Banking Security Guidelines

Account and Access Security

> Check your transaction history and statements to make sure there are no unauthorised transactions on any of your accounts

> Check your transaction history each time you update your passbook, or log on to iBank, mBank or Hume Connect

> Do not allow strangers to transact through your account for their own purposes

> Do not accept money for allowing others to transact through your account

> Set strong passwords and change them regularly

> Create passwords with letters and numbers that cannot be easily attributed to you

> Always memorise your password or PIN and do not write it down or store it on your computer

> Report any unauthorised use or suspected unathorised use

Protect your Passbook or Chequebook

> Keep your passbook and chequebook in a safe place and under your control

> Do not keep your chequebook or passbook with any card or driver's licence containing your signature

> Do not sign blank cheque forms – all details should be completed before you sign a cheque

Internet, Mobile and Phone Banking Security

> When accessing iBank or mBank, always go via Hume's main website; never store your online banking page in your favourites

> Always access Hume's website by typing the address into the browser; never log on by clicking a link embedded in an email

> When internet banking, use a security token or mobile token which can be downloaded on your mobile

> Keep your external transfer limit to the minimum required

> Never send money to someone you don't know or trust

> Check that your data is encrypted by looking for the verisign secured symbol

> Always log out from iBank or mBank and close your internet browser when finished

> Never respond to an email or phone call asking for your PIN, password or account details (Hume will never ask for these details)

> Avoid any 'pop up' windows that direct you to another website and asks you for your customer identification or password

> Avoid using publicly shared WiFi networks

> Utilise the lock capability on your mobile when it is not in use. This function helps you protect your device and details.

Protect your Computer

> Only use a trusted and secure computer to access your internet banking

> Avoid using publicly shared computers, such as those in internet cafes

> Ensure you install security software and update it regularly

> Keep your computer software up to date

> Turn on automatic updates so all of your software receives the latest fixes

> Do not click on links or open email attachments from unknown sources

> Scan your computer with anti-virus software at regular intervals

> Delete spam and hoax emails, as they can carry viruses and other malicious software

> Clear cookies and old files on a regular basis and scan for viruses, worms, Trojans etc