

- Ensure that the padlock at the bottom of the screen is present before you enter your login details
- Select a password that is difficult to guess and has no connection to you
- Never respond to an SMS or email that requests your account details and passwords. If this occurs you should advise IMB immediately and then delete the SMS or email
- Regularly change your password and device access codes
- Regularly check your account transactions and report any unauthorised transactions immediately to IMB
- Notify IMB immediately if you believe your password or account has been compromised
- Avoid using computers at public places, such as Internet Cafes
- Refer to IMB's website periodically for security updates and alerts
- Never store passwords on your smartphone, computer or other access device
- Utilise the lock capability on your mobile device when it is not in use
- Never disclose your account number, member number or access code via email or text message.
- You must not provide third parties with remote access to devices used to access IMB internet banking or mobile app, or that have IMB internet banking login credentials saved.

**Remember: IMB will never ask you to disclose your access code (such as your password for Internet Banking, One Time Passwords or Two Factor Authentication codes) or send a request to you with a link to our Internet Banking system, requiring you to enter your member number and access code for verification purposes. You may be held liable for any fraud losses where you have disclosed your PIN or access codes, or you have directly or indirectly provided or facilitated remote access to your device.**

### Liability

This section provides guidelines in relation to your liability for unauthorised transactions. Please note, however, that liability for losses resulting from unauthorised transactions are ultimately determined in accordance with the ePayments Code, rather than these security guidelines or the IMB Member Guide to Transaction Banking – Product Disclosure Statement.

You will be liable for losses where:

- IMB can prove on the balance of probabilities that you contributed to the loss through fraud or breaching the access code security requirements, with the following exceptions:

- losses incurred on any one day that exceed any applicable daily or periodical transaction limit;
- losses that exceed the balance of the facility, including any prearranged credit;
- losses incurred on any facility that IMB and you had not agreed could be accessed using the card, access device or access identifier/access code used to perform the transaction
- You provided access to IMB services by sharing biometric access
- More than one access code is required to perform a transaction and IMB can prove that you breached the access code security requirements outlined above for one or more, but not all required access codes, BUT ONLY IF IMB can prove that the breaches of the access codes security requirements were more than 50% responsible for losses when assessed together with all the contributing causes
- You contributed to the loss by leaving a card in an ATM (as long as the ATM incorporated reasonable safety standards that might mitigate the risk of a card being left in the ATM)
- IMB can prove that you contributed to the loss by unreasonably delaying reporting a security compromise – namely the misuse, loss or theft of a card or access device or that the security of all access codes has been breached
- Actual losses that occur between when you became aware of the security compromise, or, should reasonably have become aware in the case of a lost or stolen card or access device, and when the security compromise was reported to IMB. BUT you will not be liable for:
  - losses incurred on any one day that exceed any applicable daily or periodical transaction limit;
  - losses that exceed the balance of the facility, including any prearranged credit;
  - losses incurred on any facility that IMB and you had not agreed could be accessed using the card, access device or access identifier/access code used to perform the transaction
- An access code was required to perform a transaction and none of the above apply. You will be liable for the lesser of \$150; the balance of the facility/ies which IMB and you have agreed can be accessed using the card, access device and/or access code, including any prearranged credit, or the actual loss at the time that the misuse, loss or theft of a device or breach of the security of the access code is reported, excluding any portion of loss incurred on any one day that exceeds the relevant daily or periodical transaction limit.

### IMB Online Communications

From time to time, IMB may communicate with you in various ways via online channels such as emails, SMS, Live Chat, and messages in our online application systems. This may also include an SMS or email to verify your identity when making online purchases or to confirm certain transactions that have occurred on your account. It is important to remember that:

- IMB will not send emails which provide links to take a member directly to IMB's Internet Banking system
- IMB will never request passwords, PINs or answers to security questions via email
- IMB will never request your account numbers or member number via email
- IMB will never ask you to provide remote access to your devices
- IMB will not publish private information in unsolicited emails
- Members can communicate securely via our Live Chat or within the Secure Email facility contained within IMB's Internet Banking.

**If at any time you are unsure of an email you receive from IMB, please call us on 133 462.**

### IMB Contact Numbers

IMB Visa Card or Cashcard:	<b>133 462</b>	Mon to Fri 8am-8pm Sat 9am-4pm
	<b>1800 252 730</b>	(After hours)
	<b>+61 2 4298 0111</b>	(Outside Australia)
<hr/>		
IMB MasterCard:	<b>1300 135 538</b>	
	<b>+61 2 8225 0620</b>	(Outside Australia)

You should contact IMB immediately if you suspect fraud or identify any unauthorised transactions. If IMB is not contacted within a reasonable time frame we may not be able to recover the full amount of any loss.

### For more information

Pop into a branch or call us on **133 462**

Download our App or visit **imb.com.au**

For further information on security, please consider the Product Disclosure Statement available from IMB branches, by calling us on 133 462 or by writing to us at IMB Member Services, PO Box 2077, Wollongong NSW 2500. IMB Ltd trading as IMB Bank. ABN 92 087 651 974. AFSL/Australian Credit Licence 237 391. IMBSEC230505

## How to Stay Secure

Protect yourself and minimise the risk of fraud or scams.



IMB Bank has prepared this brochure to provide you with some guidelines on how to safeguard your IMB Cards, PINs, access codes and mobile devices to assist you in preventing unauthorised or fraudulent activity on your accounts.

The security of your card, access code and/or PIN, and the cards, access codes and/or PINs of additional cardholders is very important. You must make every effort to ensure that your card and access code is not misused, lost or stolen. If you fail to observe the security requirements set out in the IMB's Member Guide to Transaction Banking Product Disclosure Statement you may incur increased liability for unauthorised use of your card, access code or PIN.



### Card Security

You are responsible for the security of your card and keeping it secure at all times. This includes a digital version of a card that you have provisioned into a digital wallet on a mobile device.

To help protect your card YOU must:

- Sign the card as soon as you receive it
- Regularly check that you still have your card in your possession
- Never give your card to anyone else to use, including friends or family members (even if the account is held in joint names)
- Never provide others with access to your device where your digital card is stored
- Never share your device's PIN, access code or other password with others or allow others to register their biometric identifier (such as a fingerprint) on your device
- Not load your digital card onto another person's device
- Ensure that your contact details held by IMB are up to date
- Do not share your card details via any unsolicited SMS or email links
- Keep your devices safe, secure and locked when not in use. Only use Wi-Fi hot spots that are reputable and password protected
- Not leave your card or device where your digital card is stored unattended, for example in your car or handbag, at the beach or at work
- Always retrieve your card whenever you use it to make a purchase or for an ATM transaction
- Be aware of people standing close by to ensure that you cannot be observed entering your PIN when using an ATM or EFTPOS machine
- Do not accept any offer of assistance at an ATM or EFTPOS machine from a person unknown to you
- If you suspect that an ATM has been tampered with, do not use the ATM and advise IMB immediately
- If you become aware that your card has been lost or stolen, or been used by someone else - immediately block or cancel your card via the Mobile Banking App or Internet Banking, by calling 133 462 or visiting a branch.

If you no longer use or require your card, please notify IMB and destroy the card immediately by cutting it into small pieces, ensuring you cut the microchip and disposing of the pieces securely. If you no longer use or require your card on a mobile device, please remove the digital card from the device.

**IMB cardholders have access to Visa Secure and Eftpos Secure. These are free services that provide you with extra protection when you shop online with participating merchants using your IMB Visa Debit Card. Further information is available at [www.imb.com.au/secureshopping](http://www.imb.com.au/secureshopping)**

### Access Code and Biometric Security

Access code means your personal access code or password or any other similar information issued to you by IMB which may be required in order to access your accounts and which is required to be kept secret.

This includes, but is not limited to, PINs and your Internet Banking password, teleservices password, One Time Passwords and SMS 2FA or Two Factor Authentication mechanisms.

To protect your access codes:

- Memorise them and destroy our letter telling you your access code
- Do not select a numeric access code that represents your date of birth or the date of birth of someone close to you, or an alphabetical access code that is a recognisable part of your name or the name of someone close to you
- Never disclose your access code or make it available to any other person (including a family member or friend)
- Never record your access codes on your device, electronic equipment or anything that you carry with your device or that is liable to be stolen with your device without making a reasonable attempt to protect the security of the access code
- Do not allow any other person to register fingerprints, facial recognition or other biometric controls on your devices
- Never share One Time Passwords or Two Factor Authentication codes with anyone else
- Never allow remote access to your devices used to access IMB Internet Banking or mobile app, or that have IMB Internet Banking login credentials saved.

You must not act with extreme carelessness in failing to protect the security of all access codes. For example storing a user name and access code for internet banking in a diary, or a device that is not password protected under the heading "internet banking codes".

### What is NOT a reasonable attempt to disguise an access code

If you record your access code you must make a reasonable attempt to disguise it. The following are examples of what is NOT a reasonable attempt to disguise your access code:

- Recording your access code as a telephone number or part of a telephone number
- Recording your access code among other numbers or letters with any of them marked to indicate the access code
- Recording your access code (in sequence or disguised format) and describing it as an access code, or in any way that can be linked to your card or electronic banking (e.g. IB code 0000 or IMB code 0000).



**Notify IMB immediately if you become aware that your access codes have been lost or stolen or become known or used by someone else. In the event that IMB needs to contact you, we will do so by telephone, mail or secure email which can only be accessed once you have signed into Internet Banking.**

### Want to select your own PIN?

If you don't want to use the PIN that was provided with your IMB Visa or Cashcard, you may select one of your own at an IMB ATM, via the Mobile Banking App or Internet Banking. When selecting your PIN, it is important to remember that you should not use any of the following:

- date of birth
- car rego numbers
- licence numbers
- family members' names
- personal telephone numbers
- a number or word that can be easily guessed or associated with you
- consecutive numbers or numbers that form a pattern

You may be held liable for any fraud losses where you have selected any of the above for your PIN.

### Internet & Mobile Security

While accessing digital services, IMB will collect information and review your device logs to determine if the transactions are authentic for fraud prevention purposes. If you opt out of providing this information, your experience may be impacted as we may not be able to confirm the authenticity of your activity.

To protect your personal information and identity, it is critical that you take extra care. Here are some tips from IMB:

- Only log into IMB's Internet Banking from [www.imb.com.au](http://www.imb.com.au) or through IMB's Mobile Banking application