DON’T GET CAUGHT OFF GUARD

Keeping your money and accounts safe.
How do you make sure your money and accounts don’t fall into the wrong hands? It all starts with securing your personal information – including:

- cards
- devices that you use to make payments (these may include your smartphone, tablet or wearable device)
- Personal Identification Numbers (PINs)
- phone passcodes
- Pattern Lock codes
- Internet Banking passwords
- online account passwords
- SMS and Security Codes

**Card and device security**

- Sign the back of new cards as soon as you get them.
- Don’t let anyone else use your card.
- Regularly check that you still have your card and device.
- Let us know as soon as you realise your card or device or PIN has been lost, stolen or used by someone else.
- Don’t use a payment device if you think something isn’t right – fraudsters can use fake equipment to steal cards or capture PIN details.
- When your card expires, destroy it by shredding or cutting it up. Make sure you slice through the embedded microchip, magnetic strip and security code.

**Keeping your banking information secure**

- Don’t share your passwords, PINs or passcodes with anyone. We recommend accessing NAB’s website by typing nab.com.au into your browser, rather than from a link in an email, SMS, a pop-up window, or from your browser history.
- When transacting with NAB online, make sure your internet session is secure – check that the URL (web address) has ‘https’ at the start, and a closed padlock icon.
- Make your password/PIN hard to guess. Don’t choose a password/PIN that’s easily identified with you (e.g. your birth date, car registration, telephone number or name).
• Never write passwords or PINs down. Change them frequently.
• Use a different password/PIN for each of your online accounts.
• Don’t let anyone watch you enter your NAB Internet Banking password, or your PIN at an ATM.
• Don’t share your Visa Secure one time passcode with anyone, unless you are completing an online purchase that you initiated.
• If you have your fingerprints or Face ID saved to your phone, you can use them to login to the NAB app. To set up Touch ID or Face ID, go to Settings and select ON for Touch ID or Face ID. You should only set up Touch ID or Face ID if only your fingerprints or face image are saved on the device. If you do save someone else’s prints or image, they will be able to access your account information and change some of your settings and payment limits. That means your liability of unauthorised transactions may be affected.
• Treat your device like your wallet or purse. Keep it close at all times.

If the guidelines above are not followed, you may be liable for any unauthorised transactions.

**Avoiding scams and hoaxes**

• Treat any unsolicited emails, SMS or phone calls with caution. We’ll never send an email or SMS with a link or attachment asking you to provide personal or banking details. If you do receive a message of this nature purporting to be from ‘NAB’, don’t act on it. Instead, forward the message to phish@nab.com.au and then delete it. Alternatively, you can forward suspicious SMS to 0476 220 003.

• If you feel like a call might not be genuine, hang up, and call back on an official phone number to verify the call was legitimate (the general NAB number is listed on this brochure, on the back of your cards and online). Never provide personal information or allow the caller to have remote access to your computer on unsolicited calls.

• We’ll SMS you one-time passcodes for Internet Banking transactions, password resets and your requests for Open Banking data sharing – so it’s
important to keep your phone secure. These messages should not be shared with anyone, even NAB. If you call NAB, we may send you an identification verification SMS. This is the only code we will ask you to provide to us.

- If your mobile phone ever stops working, get in touch with your service provider to make sure you haven’t been a victim of ‘mobile phone porting’. This is where scammers may use your information to transfer your phone number to another provider so they can intercept SMS passcodes sent to you.

- When downloading Apps, ensure that they are from official App stores (App Store or on Google Play). Never download an App from a link in an email or SMS.

- Regularly check your account statements. If you spot a transaction you don’t remember or recognise, let us know straight away.

- Install up-to-date anti-virus software on your devices to detect and prevent online attacks. NAB offers customers 6-months free security software. Visit nab.com.au/software

- Avoid using computers in public places like Internet cafes, hotels and airport lounges to do online banking.

- Only bank on trusted devices and on trusted Wifi networks. Never accept a request to download a program or certificate to your device in order to use a public Wifi network.

- Regularly check your Open Banking data sharing permissions in Internet Banking (when you’ve requested for your banking data to be shared with an accredited third party). If you spot a consent you don’t remember or recognise, call us straight away.

- Report any scams to the Australian Federal Government’s SCAMWatch service at scamwatch.gov.au

- Keep up-to-date with online threats and advice at nab.com.au/security, or the Australian Federal Government’s free Stay Smart Online Alert Service. Sign up at staysmartonline.gov.au

App Store is a trademark of Apple Inc., registered in the U.S. and other countries.

Google Play and the Google Play logo are trademarks of Google LLC.
Reduce the risk of identity theft

- Secure your letterbox with a lock to prevent your mail being stolen.
- Let us know straight away if your address or contact details change.
- Never give out personal information to people you don’t know or trust.
- Don’t publish confidential information about yourself on social media, including your full name, date of birth, address or phone number – criminals can use this information to impersonate you.
- Shred documents containing your personal information before throwing them away.

When to notify NAB

If your card, phone or device has been lost or stolen, call us immediately on 1800 033 103 (within Australia) or +61 3 8641 9121 (from overseas) 24 hours, 7 days a week. (Calls from mobile phones are charged at applicable mobile phone rates.)

You can also block, unblock and replace your linked personal and business cards by clicking on My cards on the main menu in the NAB Internet Banking or the My cards menu in the NAB app.

If you believe something isn’t right with your account, let us know straight away. Call the numbers listed above if you have concerns about your card or the numbers listed on the back of the brochure for account concerns, especially if:

- Someone finds out your PIN, passcodes or passwords.
- There’s an error, unauthorised access or unauthorised transaction on your account.
- Your mobile phone is lost or stolen – and your mobile phone number is registered for SMS Security.
- You’ve provided your banking details to an unsolicited email or unknown caller.

Call us to tell us about any changes to your address.

For NAB Traveller Card call 1800 098 231 (within Australia) or +44 207 649 9404 (if overseas).