Fact Sheet

NORTHERN TERRITORY CONSUMER AFFAIRS

DATA BREACHES

What to do if your personal information is stolen in a data breach

In recent years, several significant data breaches have occurred involving major Australian companies, resulting in the theft of customer information.

Stolen personal data can be used in a range of criminal activities, leaving individuals vulnerable to identity theft and financial fraud.

This fact sheet outlines the steps you can take to protect yourself and minimise the risk of being targeted by scammers.

Stay Vigilant

If you've been affected by a data breach, be on high alert for suspicious contact. Scammers may try to contact you via phone, SMS, email or social media.

🚫 Do not click on any suspicious links or open attachments.

🔒 Never share your personal or banking information with unverified sources.

Secure Your Devices and Back Up Data

Keep your devices up to date with the latest software and security updates.

💾 Regularly back up your important data so it can be recovered in case of loss or theft.

Use Multi-Factor Authentication

Enable multi-factor authentication (MFA) on all online accounts. MFA requires two or more verification steps (e.g. a password and a code sent to your phone) before access is granted, offering extra protection against hackers.

Monitor Your Bank Accounts

Notify your bank if a data breach has impacted you. Regularly review your account statements and report any

suspicious transactions immediately.

Contact your bank or financial institution.

Let them know you may be at risk due to a data breach. Ask them to:

- Put a note on your file about potential fraud
- Watch for unusual activity
- Cancel and reissue cards if needed
- Set up transaction alerts if they're not already active

The earlier your bank is aware, the faster it can act if something suspicious happens.

Request a credit report and consider a credit ban

A criminal with your personal information might try to take out loans or credit in your name.

Contact one of the three major credit reporting agencies (Equifax, illion or Experian) to request a free credit report.

If you're concerned, ask for a temporary credit ban. This prevents anyone (including scammers) from applying for credit in your name while it's in place.

Be alert for scams - don’t click on links or give out info

After a breach, scammers may pretend to be from the company that lost your data. They might:

- Send fake emails asking you to "verify your account"
- Text you with "security updates" or "refund links"
- Call pretending to be from your bank, ATO, or a service provider

Don’t trust any unexpected messages. Contact the company directly using details from their official website;

never click a link or use contact details sent in an email or text.

Watch for strange activity on your accounts

- Bank statements for unfamiliar purchases
- Email for unusual login alerts or password resets
- Online shopping accounts (e.g. eBay, Amazon) for orders you didn't make
- If you spot anything unusual, report it immediately and change your password for that service.

Get help if you think your identity has been misused

If you suspect your personal details have been misused:

- Contact IDCARE (Australia's national identity and cyber support service):
    - www.idcare.org or 📞 1800 595 160
- Report it to the police. Keep a record of what's happened.
- Report any scams to Scamwatch: www.scamwatch.gov.au

Learn more and stay informed

The Office of the Australian Information Commissioner (OAIC) has information about how businesses must respond to breaches: www.oaic.gov.au/privacy/data-breaches