Optus Data Breach

If you think you may be affected by the recent Optus data breach **contact Optus Customer service on 133 937**. For more information, see Optus Data Breach.

You should also:

- Secure and monitor your devices and accounts for unusual activity, and ensure they have the latest security updates.

- Enable multi-factor authentication for all accounts.

- If you need assistance with taking these steps, please visit cyber.gov.au.

Be alert for scams referencing the Optus data breach. Learn how to protect yourself from scams by visiting www.scamwatch.gov.au.

If you are concerned that your identity has been compromised or you have been a victim of a scam, contact your bank immediately and call IDCARE on 1800 595 160.

If your identity has been stolen, you can apply for a Commonwealth Victims' Certificate.

If you believe you are victim of a cybercrime, go to ReportCyber at cyber.gov.au.

The following websites can help you protect yourself and stay informed:

- Identity theft | Moneysmart

- Identity fraud | OAIC

- cyber.gov.au

If you wish to make a privacy complaint, please contact Optus. If you are unable to resolve your complaint with Optus, you may wish to lodge a complaint with the Telecommunications Industry Ombudsman and the Office of the Australian Information Commissioner.

What is the Government doing to protect your identity?

The Government is looking at all possible solutions to protect and reissue victims' identity documents.

The Australian Federal Police (AFP) has launched Operation HURRICANE to investigate the criminal aspects of the breach. The AFP has also launched Operation GUARDIAN, under the APF-led JPC3, a joint partnership with law enforcement, the private sector and industry to combat cybercrime. Operation GUARDIAN is focused on shielding affected customers, where they can be identified, and working with industry to enhance protections for members of the public. The AFP is also monitoring online forums, including the internet and dark web, for criminals trying to exploit the breached data. The AFP will not hesitate to take action against those who are breaking the law.

The Australian Cyber Security Centre is supporting Optus with a cyber security incident response and assisting other Australian telecommunications providers to enhance their cyber security.

The Department of Home Affairs is working with Commonwealth, state and territory agencies to minimise the potential for exposed documents to be used fraudulently.

If your Medicare card details have been exposed, Services Australia will allow you to replace your Medicare card for free. If you believe there has been unauthorised activity to any of your Services Australia accounts, contact their Scams and Identity Theft Help Desk.

Passports are still safe to use for international travel. However, the Government understands impacted Optus customers may be concerned about identity theft relating to their passports. Customers who choose to replace their passports can call the Australian Passport Office where staff are ready to assist. Optus has agreed to reimburse the costs associated with replacing a passport due to the breach. More information can be found at www.passports.gov.au.

The Government will continue to update this factsheet as Optus provides more advice.