Optus Data Breach

As at: 20 October 2022

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 Scamwatch.

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 Government has amended the *Telecommunications Regulations 2021* to better protect Australians following the Optus data breach. They will allow Optus to share limited information with financial institutions and Government agencies to detect and mitigate the risks of malicious activity, including ID theft and scams. These changes will reduce the impact of this data breach on Optus customers and enable financial institutions and Government agencies to implement enhanced safeguards and monitoring.

The Department of Home Affairs has established a Commonwealth Credential Protection Register to help stop compromised identities from being used fraudulently. The Register will prevent some compromised identity credentials from being verified through the Document Verification Service.

The Document Verification Service is used by some government agencies and businesses, such as banks, to verify an individual's identity online. You will be notified by the credential issuer when you have been placed on the Register.

The Commonwealth Credential Protection Register will prevent credentials on the Register from being used fraudulently, such as taking out loans or setting up accounts. However, this means rightful owners will not be able to use these credentials to verify their identity online, and other credentials will be required to prove who they are. New credentials issued following the data breach will work as normal.

It is important to remain vigilant and continue to monitor your accounts for unusual activity. Some government agencies and businesses don't use the Document Verification Service and won't be protected by the Register.

In the interim, impacted individuals should consider using alternative credentials or speak to service providers that ask for identification for other options, such as visiting the service in person to present the credential.

As Optus provides data, the issuing agencies will assess it and determine whether to add credentials to the Register. As at 14 October 2022, the Register includes around 100,000 Australian Passports. These passports can still be used for international travel.

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 or Centrelink concession card details have been exposed, Optus will contact you directly. Services Australia will allow you to replace your Medicare card for free. Services Australia has also put in place additional security measures to protect your information. If your Medicare or Centrelink account has been compromised, you can call Services Australia's Scams and

Identity Theft Help Desk on 1800 941 126. They can help secure your accounts if they have been compromised.

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. Optus has agreed to reimburse the costs associated with replacing a passport due to the breach. Customers will need to pay for their replacement passport upfront and then seek a reimbursement from Optus. For more information go to Cyberattack Support (optus.com.au) or contact Optus customer service directly on 133 937.

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