FACT SHEET

Response Fact Sheet – Optus Data Breach

Background

Following a cyberattack, Optus is investigating the possible unauthorised access of current and former customers' information.

Optus has advised the information potentially exposed may include customers' names, dates of birth, phone numbers, email addresses, and, for a subset of customers, addresses, and ID document numbers such as driver licence or passport numbers. **Payment detail and account passwords have not been compromised.**

Optus has advised that customers that had the most fields exposed would be contacted first over the next few days. It is likely that if you are not contacted by Optus in the next few days, that you are not in this cohort of individuals.

Please note that notification from Optus is occurring via email and Optus will not provide any links in email or contact you via sms or phone call asking you to verify any personal details or billing information. If you are contacted via SMS or phone, do not engage, contact Optus directly through a verified point of contact.

Response Considerations

IDCARE is unable to advise, on case-by-case basis, the extent of personal information or identity credentials that have been compromised through this breach.

As a precautionary measure there are proactive response actions we recommend that you may wish to consider.

Remain vigilant about scams and unsolicited calls, emails and text messages.

- Scammers often impersonate government and businesses. Never respond to requests to provide personal and account information, or access to your device.
- Make sure you disconnect and make your own enquiries.
- Never click on any links that look suspicious or provide passwords, personal or financial information
- Consider subscribing to www.scamwatch.gov.au for the latest information about scams impacting our community.
- Look out for any suspicious or unexpected activity across your online accounts and report any fraudulent activity immediately to your provider

Wherever possible it is always recommended that any accounts you have in place are protected with multi-factor authentication.

- Talk to your account providers as to whether this security measure is available

Get your free credit reports

- Your credit reports provide a means to assess whether someone has attempted to obtain credit in your name. It is important to obtain your credit report from all three agencies as some may gather credit information others have missed.
- In Australia, you can obtain a free credit report every three months, or more often if you have been refused credit within the last 90 days, or your credit-related personal information has been corrected. To apply for your credit reports from Equifax, illion and Experian, please see IDCARE's Fact Sheet on Credit Reports Australia.

FACT SHEET

Apply for a Credit Ban with Equifax, illion and Experian (Australia)

- We recommend applying for Credit Bans with Equifax, illion and Experian (to do this please see IDCARE's Fact Sheet on Credit Bans Australia). Note that you can arrange a ban across all three Credit Reporting Agencies through one application with one of the individual agencies.

If you believe your Optus account has been compromised, contact Optus via My Optus app – which remains the safest way to contact Optus, or call on 133 937.

If you identify that you have experienced any misuse of your credentials, please contact IDCARE for support https://www.idcare.org/contact/get-help.

Information Relied Upon, Assessment Limitation & Disclaimer

In reaching our advice, IDCARE has assumed that the information communicated to IDCARE about this incident is accurate and reliable. IDCARE reserves the right to adjust our responseshould further information become available.
IDCARE provides identity and cyber security incident response services (the Services) in accordance with the following disclaimer of service:

1. IDCARE is Australia national identity and cyber incident community support service. IDCARE is a not-for-profit and registered Australian charity.
2. The Services provided do not constitute legal advice. IDCARE recommends that you consult asolicitor in relation to your legal rights and obligations, including but not limited to your legal rightsor obligations under Australian and international privacy and data protection laws.
3. To the extent the Services are based on information and documents that you have provided,IDCARE has not verified the accuracy of the information and documents and accepts noresponsibility for the accuracy of the information and documents.
4. While every effort has been made to ensure the accuracy of the information in this HarmAssessment, to the maximum extent permitted by law all conditions, terms, representations, andwarranties (in each case, whether express or implied) in connection with the provision of theServices which might otherwise be binding upon IDCARE are excluded.
5. IDCARE'S liability for any loss or damage suffered by any person or organisation (including, withoutlimitation, any direct, indirect or consequential loss or damage) arising out of or in connection withthe Services (including without limitation liability for any negligent act or omission, or statement,representation or misrepresentation of any officers, employees, agents, contractors or consultantsof IDCARE) shall be limited to the fees paid by you to IDCARE in respect of the Services. For theavoidance of doubt, this limitation of liability extends to any liability arising from any actions performed or not performed as a result of any recommendations made in the course of providingthe Services.

The Services provided by IDCARE are intended to be provided solely to inform persons who may be impacted by this incident and will not be liable to any other person who may receive this document.