



## Monthly Information Newsletter – Tax & Super

October 2022

### Optus data breach

Following a recent cyber-attack, Optus customers are advised they could be at risk of identity theft.

While Optus has not yet revealed how many of its 9.7million customers were impacted, they did confirm that the number was “significant”. Importantly, the breach has affected past Optus customers back to 2017, as well as current customers. Customers who have been affected will have already been contacted by Optus, or will be in the coming days.

Customer information that was accessed included:

- Names
- Dates of birth
- Phone numbers
- Email addresses
- Street addresses
- Drivers licence details
- Passport numbers.

However, payment details and account passwords reportedly have not been compromised and Optus’s phone services remain safe to operate. Thus, customer financial details were not directly compromised.

Of concern (not just for Optus customers, but for any person whose above information has fallen into the wrong hands) is that the above details are easily enough to compromise a person’s identity, warns the Office of the Australian Information Commissioner:

*Your identity can be stolen if a thief accesses your personal information, including from any document that contains information about you, the OAIC website says.*

*Even if a thief only accesses a small amount of your personal information, they may be able to steal your identity if they can find out more about you from public sources. This includes social media accounts which may include your date of birth, photos and information about your family.*

*Identity fraud can result in someone using another individual’s identity to open a bank account, get a credit card, apply for a passport or conduct illegal activity.*

The government’s Scamwatch website advises the following steps to protect your personal information:

- Secure your devices and monitor for unusual activity
- Change your online account passwords and enable multi factor authentication for banking
- Check your accounts for unusual activity such as items you haven’t purchased
- Place limits on your accounts or ask your bank how you can secure your money
- If you suspect fraud you can request a ban on your credit report.

Moving forward, also be vigilant regarding future contact. Scammers may use your personal information they have obtained to contact you by phone, text or email. Never click on links or provide personal or financial information to someone who contacts you out of the blue.

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. IDCARE is Australia’s national identity and cyber support service, to get expert advice from a specialist identity and cyber security service. You can also report scams to Scamwatch [www.scamwatch.gov.au](http://www.scamwatch.gov.au) and check [cyber.gov.au](http://cyber.gov.au) for information about cyber security.

Optus customers can also contact Optus directly via the My Optus app or call 133 937. Businesses can ring 133 343.

#### DISCLAIMER

All information provided in this article is of a general nature only and is not personal financial or investment advice. Also, changes in legislation may occur frequently. We recommend that our formal advice be obtained before acting on the basis of this information.

***Our liability may be limited by a scheme approved under Professional Standards Legislation.***