

Eva Lawler

Minister for Infrastructure, Planning and Logistics



Media Release

New driver's licences for impacted Optus customers

28 September 2022

The Northern Territory Government is working with Optus to assist customers whose personal data may have been compromised.

Optus advises that the number of Northern Territory customers whose driver's licence data has been stolen is around 20,000 – all people impacted will be contacted by Optus.

NT driver's licences include two key unique identifiers (Licence and Card numbers). Both are required for the licence data to be used to conduct identity fraud. The number of customers from whom the combination of key identifying numbers were stolen is expected to be about 1% (around 200 Territorians). This number will be confirmed within the next 24 hours.

Optus will advise NT customers from whom both numbers have been stolen **and strongly encourage them to apply to have their licence cancelled and re-issued.**

However we understand the remaining customers who had only their licence number stolen may also be feeling concerned. If so, you are also welcome to have your licence cancelled and re-issued.

Breach notices for impacted customers will need to be presented when obtaining a new licence.

New licence fees for impacted Optus customers will be waived by the NT Government.

Quotes from the Minister for Infrastructure, Planning and Logistics, Eva Lawler:

"Protecting the personal details of Territorians is paramount in this case.

“The Territory Government is very aware of the anxiety this breach has created for Optus customers and we are doing what we can to help address the issue.

“We can assist through prioritising licence replacements for affected residents and waiving fees.”

Q&As

I am an Optus customer – how do I know if my licence data has been stolen?

- Optus estimates approximately 20,000 NT customers have had their licence data compromised.
- The telco will be contacting customers to advise if they have had one or two identifying numbers breached.
- Customers can also check the [Optus website](#) for information and contact Optus via the My Optus App or call 133 937.

How are two identifying numbers necessary for identity fraud?

- NT driver’s licences each carry two numbers: the licence number which appears on the front of your licence, and the card number, in small print on the back of the licence. The licence number is your authority to drive. The card number is unique to the physical licence that you carry.
- Both the licence number AND the card number are required for identity fraud.

I provided my licence number but not my card number – do I need a new licence?

- Both the licence number AND the card number are required for identity fraud. It is not necessary to seek a new licence.
- If you wish, you can contact MVR and arrange for a new card to be issued. There is no charge for Optus customers.

Do I have to pay for a new licence?

- Optus customers who require new licences will not be charged. <https://nt.gov.au/driving/mvr-services>

Do I need to attend the Motor Vehicle Registry in person to get a new licence?

- Affected customers will have to attend an MVR and present their notice from Optus. Regional and remote clients should contact the MVR on 1300 654 628 (Monday-Friday, 8am-4pm).

What do I need to do to protect my identity?

- All Optus customers are urged to remain vigilant and report any suspicious activity to 133 937.
- Scammers often impersonate government and businesses. Never respond to requests to provide personal and account information, or access to your device.
- 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.
- Further information for Optus customers is available at <https://www.oaic.gov.au/updates/news-and-media/advice-on-optus-data-breach>