s. 22(1)(a)(ii)

Subject: Optus CEO and MHAO call
Location: Teleconference - details circulated via text from Soph

Start: Wed 28/09/2022 12:00 PM
End: Wed 28/09/2022 12:30 PM

Recurrence: (none)

Organizer: Clare O'NEIL

Categories: External Meetings

s. 22(1)(a)(ii)

Subject: Call CEO Optus
Location: Teleconference - details circulated via text

Start: Mon 26/09/2022 7:20 PM
End: Mon 26/09/2022 7:50 PM

Recurrence: (none)

Organizer: Clare O'NEIL

Categories: External Meetings

From: s. 22(1)(a)(ii)
To: Clare O"NEIL
Subject: Fwd: Optus request for assistance[SEC=OFFICIAL]
Date: Sunday, 25 September 2022 12:32:49 PM
Attachments: 25092022 - Govt direction to assist - Protecting Optus Customers.pdf

---

OFFICIAL

Sent by Email+

OFFICIAL

From: "s. 47F(1)
Date: Sunday, 25 September 2022 at 12:23:20 pm
To: "clare.oneil.s. 47F(1)
s. 47F(1)
s. 47F(1) >
Cc: s. 22(1)(a)(ii)
s. 47F(1)
Subject: Optus request for assistance

Dear Minister

Please find attached a letter from Optus CEO, Kelly Bayer Rosmarin, seeking your assistance to help us take further steps to protect our customers as a consequence of the data theft form Optus.

Kind regards

s. 47F(1)

s. 47F(1)

1 Lyonpark Road
Macquarie Park
NSW 2113 Australia
s. 47F(1)

OPTUS

The Hon Claire O'Neil MP
Minister for Home Affairs
Minister for Cyber Security
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

Dear Minister O'Neil

Protecting customers following Optus Data Theft

Further to Optus' discussions with your Office, Optus is seeking the Minister's support in taking further steps to protect current and former customers impacted by the recent data theft incident.

Following discovery of this incident, Optus has been proactive in providing early warning to all current and former customers to enable them to increase their vigilance against potential harm.

One of Optus' early actions in response to the data theft, and prior to notifying the media, was also to notify key financial institutions so they could enhance vigilance in protecting customers. s. 47G(1)(a)

s. 47G(1)(a)

s. 47G(1)(a)

Optus is mindful that any decision made regarding the sharing of customer information with financial institutions needs to carefully balance:

- What is believed to be in the public's best interest;
- The security risks in sharing information, as further proliferation of this information may not be desirable and could increase risk of exposure for customers (although appropriate safeguards could be implemented to address this); and
- The potential for negative public sentiment arising from the sharing of this information with other organisations.

s. 47G(1)(a)

Optus reiterates that the information set exposed in the cyberattack is limited. We have been public about the specific fields to allow all other organisations to assess which of their processes could be at risk. It is Optus' considered view that these specific fields would not be sufficient for financial fraud where passwords, copies of ID documents, and/or multi-factor authentication is in place.

We also believe that most financial institutions require a password or verification by email or SMS for high value transactions – none of these have been compromised and so the integrity of the financial system should be maintained. s. 47G(1)(a)

s. 47G(1)(a)

s. 47G(1)(a) Optus welcomes the Minister's guidance on what best steps can be taken in this regard.

Optus continues to communicate and update our customers, and to explore the most appropriate support and services we can provide to help them prevent fraudulent activities. We would like to thank the Minister and Department for their support in reiterating key messages related to identify protection.

Optus is grateful for the Minister's time and assistance with this matter. Should you wish to discuss this letter, please contact s. 47F(1) on s. 47F(1)

Yours sincerely,

s. 47F(1)

Kelly Bayer Rosmarin
CEO Optus

Copy to
Minister for Communications, the Hon Michelle Rowland MP
Attorney-General, The Hon Mark Dreyfus KC, MP