

GENERAL ANNOUNCEMENT::OPTUS MEDIA ALERT

Issuer & Securities

Issuer/ Manager

SINGAPORE TELECOMMUNICATIONS LIMITED

Securities

SINGTEL - SG1T75931496 - Z74

Stapled Security

No

Announcement Details

Announcement Title

General Announcement

Date & Time of Broadcast

03-Oct-2022 17:29:53

Status

New

Announcement Sub Title

Optus media alert

Announcement Reference

SG221003OTHRJ7Q1

Submitted By (Co./ Ind. Name)

Lim Li Ching (Ms)

Designation

Assistant Company Secretary

Description (Please provide a detailed description of the event in the box below)

Please see the attached media alert issued by Optus, a subsidiary of Singapore Telecommunications Limited. For more details on this incident, please see <https://www.optus.com.au/support/cyberattack>.

Attachments

[MR-20221003.pdf](#)

Total size =90K MB

Update for customers on cyberattack

Optus today provided updated information about the impact of the cyberattack on customers.

On the back of extensive ongoing engagement with more than 20 Federal, State and Territory government agencies and departments, Optus has confirmed:

- Approximately 1.2 million customers have had at least one number from a current and valid form of identification, and personal information, compromised. Optus has communicated with these customers and recommended that they take action to change their identification documents.
- In addition, approximately 900,000 customers have had numbers relating to expired IDs compromised, in addition to personal information. We continue to work with governments and agencies regarding what further steps, if any, those customers should take.

Today's update helps provide more clarity for our customers. Having worked with government agencies to meticulously analyse the data for the company's 9.8 million customers, Optus can confirm the exposed information did not contain valid or current document ID numbers for some 7.7 million customers. The data contained details such as email address, date of birth or phone numbers. For these customers, it is important to remain vigilant.

Optus has sent an email or SMS to the customers that have had current ID documents compromised in the cyberattack, advising that details from their ID documents have been compromised and what they should do. Optus also contacted customers whose ID documents had expired to notify them that ID documents were compromised.

For customers seeking more details beyond the regular updates on the [Optus.com.au](https://www.optus.com.au), other information can be obtained at [Scamwatch](https://www.scamwatch.gov.au) and [cyber.gov.au](https://www.cyber.gov.au).

Optus will continue to update customers and government agencies regularly.