9 November 2022

Medibank cybercrime update

Medibank has today become aware that the criminal has released files on a dark web forum containing customer data that is believed to have been stolen from Medibank's systems.

This data includes personal data such as names, addresses, dates of birth, phone numbers, email addresses, Medicare numbers for ahm customers (not expiry dates), in some cases passport numbers for our international students (not expiry dates), and some health claims data.

The files appear to be a sample of the data that we earlier determined was accessed by the criminal. We will continue to work around the clock to inform customers of what data we believe has been stolen and any of their data included in the files on the dark web and provide advice on what customers should do.

We expect the criminal to continue to release files on the dark web.

Over the last 24 hours we wrote to our customers to alert them to the threat from the criminal that they could begin releasing stolen Medibank customer data on the dark web and that the criminal could also attempt to contact customers directly.

Medibank is working with the Australian Government, including the Australian Cyber Security Centre and the Australian Federal Police. The Australian Federal Police is investigating this cybercrime.

Medibank CEO David Koczkar said: "We unreservedly apologise to our customers.

"This is a criminal act designed to harm our customers and cause distress.

"We take seriously our responsibility to safeguard our customers and we stand ready to support them," he said.

If you are a victim of cybercrime, you can report it at ReportCyber on the Australian Cyber Security Centre website. To report a scam, go to ScamWatch. If you believe you are at physical risk, please call emergency services (000) immediately.

Customers can also contact us via our contact centre team (13 23 31 for Medibank and international customers, 13 42 46 for ahm customers and 1800 081 245 for My Home Hospital patients).

Customers should be vigilant with all online communications and transactions including:

- Being alert for any phishing scams via phone, post or email
- Verifying any communications received to ensure they are legitimate
- Not opening texts from unknown or suspicious numbers
- Changing passwords regularly with 'strong' passwords, not re-using passwords and activating multi-factor authentications on any online accounts where available
- Medibank will never contact customers asking for password or sensitive information

The Australian Government has activated the National Coordination Mechanism to bring together agencies across the Australian Government, states and territories.

We will continue to provide updates to our customers, including at www.medibank.com.au/cybersecurity.

This page will feature our latest announcements, along with answers to frequently asked questions and further details regarding our Cyber Response Support Program.

This announcement has been authorised for release by the Board.

For further information please contact:

For media

Emily Ritchie
Senior Executive, External Affairs
M: +61 429 642 418
Email: Emily.Ritchie@medibank.com.au

For investors/analysts

Colette Campbell
Senior Executive, Investor Relations
T: +61 475 975 770
Email: investor.relations@medibank.com.au