ASX release

17 October 2022

Medibank cyber incident and trading update

- There remains no evidence customer data has been removed from the network – investigation continues
- Medibank systems detected the unusual activity consistent with the precursors to a ransomware event
- Normal business operations have resumed, and necessary action will continue to be taken to further safeguard the IT environment including customer data
- Medibank does not expect this short disruption to impact the momentum of the business

The Medibank Group today confirmed that ongoing investigations continue to show there remains no evidence customer data has been removed from its IT environment, after it detected unusual activity last week in part of its IT network.

Normal operations have resumed, and Medibank will continue to investigate the incident as part of its ongoing forensic analysis.

When the unusual activity was detected on part of its network, the company took the precautionary action to temporarily block and isolate access to the ahm and international student customer policy management systems while the activity was investigated.

This was done out of an abundance of caution, and it enabled Medibank to provide additional protection of customer data on that system.

The systems were restored on new IT infrastructure and normal activity resumed for ahm and international student business on Friday 14 October 2022.

Medibank also deployed additional security measures across its network, strengthening the integrity of its systems. Medibank has contained the ransomware threat but remains vigilant and will take necessary steps in the future to protect its operations and its customers' data.

Medibank's investigation, which is ongoing, indicated that its cyber security systems had detected activity consistent with the precursor to a ransomware event. This initial finding was shared with the Australian Cyber Security Centre, who provided Medibank with additional guidance in support of this conclusion.

Medibank systems were not encrypted by ransomware during this incident and there is no indication that the incident was caused by a state-based threat actor.

As a health company providing health insurance and health services, Medibank holds a range of necessary personal information of customers, and the protection of customers' data security is its highest priority. Medibank is continuing to work with external parties to provide them with assurance about this incident, and Medibank's recovery.

During this incident customers have continued to be able to access health services and their health providers during this time.

The Australian Cyber Security Centre (the Australian Government lead agency) was engaged and Medibank is working in an open and cooperative manner with them to both keep national response agencies updated and to receive information and intelligence which is assisting with the resolution of the incident.

In addition, Medibank has been in regular contact with its regulators, government departments and other key stakeholders.

Although there is nothing that customers need to do, Medibank and ahm customers can contact us by phone (for ahm customers 1300 573 942 and for Medibank customers 13 23 31) or visit the information page on the website (medibank.com.au/health-insurance/info/cyber-security/) for any updates.

Trading update:

During the three months to 30 September 2022, the business has continued to show good momentum and is tracking in line with the FY23 outlook as outlined in the FY22 financial results. Medibank does not expect this short disruption to impact this momentum.

Medibank CEO David Koczkar said:

"We are sorry this incident occurred, and we understand this news may have caused concerns and inconvenience for some of our customers.

"We took the necessary precautions to protect the data of our customers, people and other stakeholders, and we will continue to do so.

"I thank our customers for their patience during this incident. We take the protection of our customers' data very seriously and ongoing investigations continue to show no evidence customer data has been removed from our network. We will provide updates if the situation changes.

"I would like to thank the Australian Cyber Security Centre, regulators and government departments who have contributed to, and supported our response and worked so effectively with us.

"We will also share technical information with peers across the industry as part of our commitment to helping others understand how this incident transpired and to allow our industry peers to bolster their own defences.

"And, of course, I would like to thank our people, who throughout this incident remained focused on supporting the health and wellbeing of our customers. In particular, thank you to our frontline people who did an exceptional job in helping our customers."

This announcement has been authorised for release by The Board.

Investor briefing today:

Investor briefing details are below. Media are welcome to join the investor briefing in a listen-only mode.

Time: 9.30am AEDT

To join this call and/or ask a question, pre-register at: https://s1.c-conf.com/diamondpass/10026199-nslrwa.html

To view the webcast only, visit: https://ccmediaframe.com/?id=pHSz7qd4

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