7 November 2022

For personal use only

Medibank cybercrime update

- **Medibank will not pay any ransom demand for this data theft**
- **Medibank updates what customer information it believes has been accessed and stolen by the criminal**
- **Medibank expands Cyber Response Support Program**
- **Business operations have been maintained**
- **Medibank announces an external review of the cyberattack**

Medibank is committed to taking decisive action to protect our customers, our people, and the community in relation to the cybercrime perpetrated against its customers last month.

Medibank CEO David Koczkar said we again unreservedly apologise to our customers and recognise the distress this cybercrime has caused.

Medibank has today announced that no ransom payment will be made to the criminal responsible for this data theft.

Mr Koczkar said: “Based on the extensive advice we have received from cybercrime experts we believe there is only a limited chance paying a ransom would ensure the return of our customers’ data and prevent it from being published. In fact, paying could have the opposite effect and encourage the criminal to directly extort our customers, and there is a strong chance that paying puts more people in harm’s way by making Australia a bigger target.”

“It is for these reasons we have decided we will not pay a ransom for this event,” he said.

This decision is consistent with the position of the Australian Government.

Based on our investigation to date into this cybercrime we currently believe the criminal:

- Accessed the name, date of birth, address, phone number and email address for around 9.7 million current and former customers and some of their authorised representatives. This figure represents around 5.1 million Medibank customers, around 2.8 million ahm customers and around 1.8 million international customers
- Did not access primary identity documents, such as drivers’ licences, for Medibank and ahm resident customers. Medibank does not collect primary identity documents for resident customers except in exceptional circumstances
- Accessed Medicare numbers (but not expiry dates) for ahm customers
- Accessed passport numbers (but not expiry dates) and visa details for international student customers
- Accessed health claims data for around 160,000 Medibank customers, around 300,000 ahm customers and around 20,000 international customers. This includes service provider name and location, where customers received certain medical services, and codes associated with diagnosis and procedures administered. Additionally, around 5,200 My Home Hospital (MHH) patients have had some personal and health claims data accessed and around 2,900 next of kin of these patients have had some contact details accessed

- Accessed health provider details, including names, provider numbers and addresses
- Did not access health claims data for extras services (such as dental, physio, optical and psychology)
- Did not access credit card and banking details

Given the nature of this crime, we now believe that all of the customer data accessed could have been taken by the criminal.

Customers should remain vigilant as the criminal may publish customer data online or attempt to contact customers directly.

"We take seriously our responsibility to safeguard our customers. The weaponisation of their private information in an effort to extort payment is malicious, and it is an attack on the most vulnerable members of our community," Mr Koczkar said.

"We will continue to support all people who have been impacted by this crime through our Cyber Response Support Program. This includes mental health and wellbeing support, identity protection and financial hardship measures.

"Medibank will also commission an external review to ensure that we learn from this event and continue to strengthen our ability to safeguard our customers," he said.

Medibank continues to work with the Australian Government, including the Australian Cyber Security Centre and the Australian Federal Police.

Normal business operations have been maintained during this cybercrime event with customers continuing to access health services. No further suspicious activity inside our systems has been detected since 12 October 2022.

Medibank has prioritised preventing further unauthorised entry to its IT network and is continuing to monitor for any suspicious activity. This has included bolstering existing monitoring, adding further detection and forensics capability across Medibank's systems and network and scaling up analytical support via specialist third parties.

Medibank has drawn on multiple sources of data across its systems to reconstruct what we believe the criminal accessed, to determine the customer impact. This complex process involved our people analysing millions of records across numerous applications and matching customer data from multiple sources.

Medibank is required by law to retain certain customer (including former customer) information for particular periods of time, generally for 7 years from when a customer leaves us, but in some instances longer.

Supporting our customers

We will continue to inform affected customers of what data we believe has been accessed or stolen and provide advice on what they should do. This will be done via email or letter and in some cases via phone.

We have expanded our dedicated Cyber Response Support Program for our customers to now include:

- **A cybercrime health & wellbeing line (1800 644 325) –** counsellors that have experience supporting vulnerable people (such as those at risk of domestic violence) and have been trained to support victims of crime and issues related to sensitive health information
- **Mental health outreach service –** proactive support service for customers identified as being vulnerable, or through referral from our contact centre team

For personal use only

- **Better Minds App –** new tailored preventative health advice and resources specific to cybercrime and its impact on mental health and wellbeing, including tools for managing anxiety and fear, with additional phone based psychological support available
- **Personal duress alarms –** for customers particularly vulnerable and/or with safety risks

The program already includes:

- **Hardship support** for customers who are in a uniquely vulnerable position as a result of this crime which can be accessed via our contact centre team (13 23 41 for Medibank and international customers, 13 42 46 for ahm customers and 1800 081 245 for MHH patients)
- **Specialist identity protection advice and resources** through IDCARE's purpose-built Medibank page
- **Free identity monitoring services** for customers whose identity has been compromised as a result of this crime
- **Reimbursement of ID replacement fees** for customers who need to replace any identity documents that have been compromised as a result of this crime
- **Specialised teams** to help our customers who receive scam communications or threats

To further assist our customers, we've extended call centre hours and created dedicated specialist teams to support customers.

Reach out for support

We understand this crime will be distressing for many of our customers.

Customers should reach out for support if they need it from:

- Medibank's Mental Health Support line on 1800 644 325 (Medibank international students call 1800 887 283 and ahm international students call 1800 006 745)
- Beyond Blue (1300 224 636 / beyondblue.org.au)
- Lifeline (13 11 14 / lifeline.org.au)
- Their GP or other relevant health professional

Remaining vigilant

Medibank recommends being 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

If you are a victim of cybercrime, you can report it at ReportCyber on the Australian Cyber Security Centre website.

If you wish to report a scam or a vulnerability, go to ScamWatch.

Regular updates will continue

As we have worked through this cybercrime, Medibank has committed to being transparent as events unfold and more is understood, including how that could impact our customers, our people, and the broader community.

For personal use only

Our investigation is ongoing, and our understanding of this crime continues to evolve. Medibank will continue to provide updates as information becomes available and is verified.

Customers are also able to access updates 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.

Australian Government investigation and support

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

Medibank is working with the Australian Government, including the Australian Cyber Security Centre and the Australian Federal Police. The Australian Federal Police continues their criminal investigation.

Medibank thanks the Australian Government and its agencies for their ongoing support and assistance during what continues to be a difficult time for our customers and our people.

Medicare card replacement and protection

Services Australia has controls in place to prevent Medicare numbers being used for identity theft. Customers can replace their Medicare card through myGov or the Express Plus Medicare mobile app. Find out more at www.servicesaustralia.gov.au/medicarecard.

External review

In addition to its ongoing forensic investigations, Medibank will commission an external review to ensure that we learn from this cyberattack and continue to strengthen our ability to safeguard our customers.

Medibank will announce more details of this review in the near future.

Medibank commits to sharing the key outcomes of the review, where appropriate, having regard to interests of its customers and stakeholders and the ongoing nature of the Australian Federal Police investigation.

This announcement has been authorised for release by the Board.

For personal use only

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

Jennifer Troy
Investor Relations Manager
T: +61 488 216 253
Email: investor.relations@medibank.com