Update,  Thursday 23 February, 2023

Today we can share an outline of what happened, our customer and technology response, and the steps taken to close down the criminal’s attack path.

**What happened**

* The criminal accessed our systems using a stolen Medibank username and password used by a third-party IT service provider
* The criminal used the stolen credentials to access Medibank’s network through a misconfigured firewall which did not require an additional digital security certificate
* The criminal was able to obtain further usernames and passwords to gain access to a number of Medibank’s systems and their access was not contained
* Following the triage of a security alert on 11 October we closed down the criminal’s attack path and can reconfirm no further activity by the criminal since 12 October 2022 has been detected inside our systems.

**What we’ve done in response:**  
Our customers

* Continued to support customers through our Cyber Response Support Program
* Continue to maintain additional resources in our phone and messaging channels to continue to support customers through 2H23
* Launched additional security measures for customers who call us

Our technology

* Implemented further controls around our technical perimeter, including ensuring that the firewall authentication was fully configured across the whole network
* Bolstered existing monitoring and added further detection and forensics capability
* Successfully completed Operation Safeguard

External review/OAIC investigation

* Deloitte conducting an external review, and that review is ongoing
* Co-operating with the Office of the Australian Information Commissioner in its formal investigation

**Our focus moving forward**

* Prioritise the support for our customers and ensure they have confidence in the protection of their data
* Continue to strengthen our security environment, which currently defends around 18 million perimeter attacks a day
* Reinforce with our people that security is everyone’s business, and uplift the security literacy of all our users
* Continue to evolve our approach to data management, particularly in light of impending reform to the Privacy Act and changing community expectations

Update,  Saturday 10 December

We can confirm that our systems are back up and running, following the successful completion of the next steps of Operation Safeguard that started Friday evening.

All customer-facing platforms have been tested with IT security experts from Microsoft and are operational with enhanced security.

**Claiming**

HICAPS is back up and running so you are able to process claims through the system.

**Eligibility checks**

Eclipse is back up and running so you are able to process eligibility checks.

Update, Thursday 8 December

Medibank and ahm systems will be temporarily offline from 8.30pm (AEDT) on Friday 9 December 2022 as we undertake some maintenance to further strengthen our systems and enhance security protections.

This is a planned operation with Microsoft and is the next necessary phase of our ongoing work to further safeguard our network. We expect the systems will be back online Sunday 11 December 2022 at the latest.

During the operation, customers won’t be able to access Medibank or ahm services through the website or app, and HICAPS won’t be available for claiming on the spot. Our retail stores and customer contact centres will also be closed Saturday 10 December 2022.

Our contact centres and retail stores will reopen on Monday 12 December 2022.

Amplar Health services such as our 24/7 critical health support lines will not be impacted by the operation.

We apologise for the inconvenience this may cause and thank you for your understanding.

Update, Thursday 1 December

We are aware that stolen Medibank customer data has been released on the dark web overnight.

We are in the process of analysing the data, but the data released appears to be the data we believed the criminal stole.

Unfortunately, we expected the criminal to continue to release files on the dark web.

While our investigation continues there are currently no signs that financial or banking data has been taken.  And the personal data stolen, in itself, is not sufficient to enable identify and financial fraud.  The raw data we have analysed today so far is incomplete and hard to understand.

Medibank CEO David Koczkar said while there are media reports of this being a signal of ‘case closed’, our work is not over.

“We are remaining vigilant and are doing everything we can to ensure our customers are supported.  It’s important everyone stays vigilant to any suspicious activity online or over the phone,” he said.

“We will continue to support all people who have been impacted by this crime through our [Cyber Response Support Program](https://www.medibank.com.au/health-insurance/info/cyber-security/cyber-support/).  This includes mental health and wellbeing support, identity protection and financial hardship measures.

“If customers are concerned, they should reach out for support from our cybercrime hotline, our mental health support line ([1800 644 325](tel:1800644325)), [Beyond Blue](https://www.beyondblue.org.au/), [Lifeline](https://www.lifeline.org.au/) or their GP.

“Anyone who downloads this data from the dark web, which is more complicated than searching for information in a public internet forum and attempts to profit from it is committing a crime.

“The Australian Federal Police have said law enforcement will take swift action against anyone attempting to benefit, exploit or commit criminal offenses using stolen Medibank customer data.  We continue to work closely with the Australian Federal Police who are focused, as part of Operation Guardian, on preventing the criminal misuse of this data.

“Again, I unreservedly apologise to our customers.

“We remain committed to fully and transparently communicating with customers and we will continue to contact customers whose data has been released on the dark web,” Mr Koczkar said.

Our customers can also contact us to understand what data has been accessed – we’ve extended call centre hours and we’ve increased our customer support team by more than 300 people.  In addition, from this week, we’re taking extra security steps to further protect our customers – with two-factor authentication in our contact centres.  So, when a customer calls for support, we can verify their identify and be sure we’re speaking with them and not someone else.

**Data released on the dark web today**

We are conducting further analysis on the files today and at this stage believe:

* There are 6 zipped files in a folder called ‘full’ containing the raw data that we believed the criminal stole
* Much of the data is incomplete and hard to understand
* For example, health claims data released today has not been joined with customer name and contact details

Given the sensitive nature of the stolen customer data that is being released on the dark web we continue to ask the media and others to support our ongoing efforts to minimise harm to customers, and not to unnecessarily download sensitive personal data from the dark web and to refrain from contacting customers directly.

Update, Monday 14 November

Given the nature of the stolen data that the criminal continues to release on a dark web forum we are in the process of contacting customers, and we urge our customers to reach out for support.

We are continuing 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.

If you are concerned, please reach out for support:

* Our dedicated [Cyber Response Support Program](https://www.medibank.com.au/health-insurance/info/cyber-security/cyber-support/)
* Medibank’s Mental Health Support line on [1800 644 325](tel:1800644325) (Medibank international students call [1800 887 283](tel:1800887283) and ahm international students call [1800 006 745](https://www.medibank.com.au/health-insurance/info/cyber-security/1800006745/))
* Beyond Blue ([1300 224 636](https://www.medibank.com.au/health-insurance/info/cyber-security/1300224636/) / [beyondblue.org.au](https://www.beyondblue.org.au/))
* Lifeline ([13 11 14](tel:131114) / [lifeline.org.au](https://www.lifeline.org.au/))
* Their GP or other relevant health professional

Because of the sensitive nature of the stolen customer data, we continue to ask the media and others to support our ongoing efforts to minimise harm to customers, and not to unnecessarily download sensitive personal data from the dark web, and to refrain from contacting customers directly.

[Read the full news item in our newsroom.](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cybercrime-update14Nov)

Update, Friday 11 November

In a statement by AFP Commissioner Reece Kershaw:

“The AFP believes that those responsible for this cybercrime are in Russia and it will be holding talks with Russian law enforcement about the individuals believed to be involved."

[Read more here](https://www.medibank.com.au/livebetter/newsroom/post/statement-by-afp-commissioner-reece-kershaw-on-medibank-private-data-breach)

Update, Friday 11 November

Given the nature of the stolen data that the criminal continues to release on a dark web forum, we are in the process of contacting customers, and we urge our customers to reach out for support.

Support is available from:

* Our dedicated [Cyber Response Support Program](https://www.medibank.com.au/health-insurance/info/cyber-security/cyber-support/)
* Medibank’s Mental Health Support line on [1800 644 325](tel:1800644325) (Medibank international students call [1800 887 283](tel:1800887283) and ahm international students call [1800 006 745](https://www.medibank.com.au/health-insurance/info/cyber-security/1800006745/))
* Beyond Blue ([1300 224 636](https://www.medibank.com.au/health-insurance/info/cyber-security/1300224636/) / [beyondblue.org.au](https://www.beyondblue.org.au/))
* Lifeline ([13 11 14](tel:131114) / [lifeline.org.au](https://www.lifeline.org.au/))
* Their GP or other relevant health professional

As part of Operation Guardian, the Australian Federal Police (AFP) have said it is an offence to buy stolen data, which could be used for financial crimes.

The AFP have also said law enforcement will take swift action against anyone attempting to benefit, exploit or commit criminal offences using stolen Medibank customer data.

[Read the full news item in our newsroom.](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cybercrime-update11Nov)

Update, Thursday 10 November

Medibank is aware that the criminal has released an additional file on a dark web forum containing customer data that is believed to have been stolen from Medibank’s systems.

We recommend remaining vigilant with all online communications and transactions including:

* Being alert for any [phishing](https://www.cyber.gov.au/learn/threats/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 contacted by someone who claims to have your data, or you are a victim of cybercrime, you can report it at ReportCyber on the [Australian Cyber Security Centre website.](https://www.cyber.gov.au/acsc/report) To report a scam, go to [ScamWatch](https://www.scamwatch.gov.au/report-a-scam). If you believe you are at physical risk, please call emergency services ([000](tel:000)) immediately.

We are supporting customers with our dedicated Cyber Response Support Program for our customers. [Find out more](https://www.medibank.com.au/health-insurance/info/cyber-security/cyber-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](tel:1800644325) (Medibank international students call [1800 887 283](tel:1800887283) and ahm international students call [1800 006 745](https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/1800006745))
* Beyond Blue ([1300 224 636](https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/1300224636) / [beyondblue.org.au](https://www.beyondblue.org.au/))
* Lifeline ([13 11 14](tel:131114) / [lifeline.org.au](https://www.lifeline.org.au/))
* Their GP or other relevant health professional

[Read the full news item in our newsroom.](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cybercrime-update10Nov)

Update, Wednesday 9 November

We have 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.

This is a criminal investigation by the Australian Federal Police.

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 passwords or sensitive information

If you are a victim of cybercrime, you can report it at [ReportCyber](https://www.cyber.gov.au/acsc/report) on the Australian Cyber Security Centre website.  To report a scam, go to [ScamWatch](https://www.scamwatch.gov.au/).  If you believe you are at physical risk, please call emergency services (000) immediately.

The Australian Federal Police has expanded Operation Guardian to protect Medibank and ahm customers and former customers whose personal information has been released by the criminals. [Read the full AFP release](https://www.medibank.com.au/livebetter/newsroom/post/afp-media-release-operation-guardian-expanded-to-protect-stolen-information).

Update, Tuesday 8 November

We are aware of media reports of a purported threat from a criminal to begin publishing stolen Medibank customer data online in 24 hours. The criminal could also attempt to contact customers directly.

We are working with the Australian Government, including the Australian Cyber Security Centre and the Australian Federal Police. The Australian Federal Police is investigating this cybercrime and trying to prevent the sharing and sale of our customers’ data.

If you are contacted by someone who claims to have your data, or you are a victim of cybercrime, you can report it at [ReportCyber](https://www.cyber.gov.au/acsc/report) on the Australian Cyber Security Centre website. To report a scam, go to [ScamWatch](https://www.scamwatch.gov.au/). 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](tel:132331) for Medibank and international customers, [13 42 46](tel:134246) for ahm customers and [1800 081 245](tel:1800081245) 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 passwords or sensitive information

We unreservedly apologise to our customers.

Update at 9:00am, Monday 7 November

Today, we’ve announced that no ransom payment will be made to the criminal responsible for this data theft.

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.

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 has accessed:

* 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
* Medicare numbers (but not expiry dates) for ahm customers
* Passport numbers (but not expiry dates) and visa details for international student customers
* 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
* Health provider details, including names, provider numbers and addresses

We believe the criminal has not accessed:

* Credit card and banking details
* 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
* Health claims data for extras services (such as dental, physio, optical and psychology)

Given the nature of this crime, unfortunately 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.

If you are a victim of cybercrime you can report it to [ReportCyber | Cyber.gov.au](https://www.cyber.gov.au/acsc/report).

How are we responding?

We acknowledge how distressing this will be for our customers and apologise unreservedly.

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
* 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:

* Mental health and wellbeing support available through Medibank’s 24/7 support line [1800 644 325](tel:1800644325) – this is available for all customers (Medibank international students call [1800 887 283](tel:1800887283) and ahm international students [1800 006 745](tel:1800006745))
* 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](tel:132341) for Medibank and international customers, [13 42 46](tel:134246) for ahm customers and [1800 081 245](tel:1800081245) for MHH patients)
* Specialist identity protection advice and resources through IDCARE’s purpose-built  [Medibank page](https://www.idcare.org/medibank-breach-response)
* Free identity monitoring services for customers whose identity has been compromised as a result of this crime
* Reimbursement of 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

As previously reported, premium increases have been deferred for Medibank and ahm customers. These were scheduled to rise on 1 November 2022, and will now occur on 16 January 2023.

Update at 10am, Friday 28 October

The ongoing investigation has now found that the criminal has accessed data that includes some My Home Hospital patient (MHH) information.

My Home Hospital is a service delivered by a joint venture between Calvary and Medibank on behalf of Wellbeing SA and the South Australian Government.

The data accessed includes some personal information (including some health data).

While Medibank has not yet determined if the information has been illegally taken from our system, we know it has been accessed.

We unreservedly apologise to our patients who have been the victims of this very serious crime.

We appreciate this will be distressing for you.

If we find your data has been stolen or accessed, we will notify you as soon as possible, which will include specific advice and support.

For more information:

[Read the latest news from the Newsroom](https://www.medibank.com.au/livebetter/newsroom/post/media-statement-medibank-cybercrime-event-and-my-home-hospital)

Update at 9.30am, Wednesday 26 October

Since yesterday’s announcement, our cybercrime investigation has now established that **the criminal had access to:**

* All ahm customers’ personal data and significant amounts of health claims data
* All international student customers’ personal data and significant amounts of health claims data
* All Medibank customers’ personal data and significant amounts of health claims data

As previously advised, we have evidence that **the criminal has removed some of this data** and it is now likely that the criminal has stolen further personal and health claims data.

As a result, we expect that the number of affected customers could grow substantially.

Our priority is to continue working to understand the specific data that has been taken for each of our customers so that we can contact them directly to let them know.

We have a comprehensive support package for customers who have had their data stolen which includes:

* Financial support for customers who are in a uniquely vulnerable position as a result of this crime. They will be supported on an individual basis.
* Free identity monitoring services for customers who have had their primary ID compromised
* Reimbursement of fees for re-issue of identity documents that have been fully compromised in this crime

And we are offering all customers access to:

* Specialist identity protection advice and resources from [IDCARE](https://www.idcare.org/medibank-breach-response)
* Medibank's [mental health and wellbeing support line](https://www.medibank.com.au/health-support/health-services/mental-health/)

For more information:

[Read the latest news from the Newsroom](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-response)

Update at 8.30am, Tuesday 25 October

Medibank has announced a comprehensive support package for our customers affected by our cyber event.

The support package includes:

* A hardship package to provide financial support for customers who are in a uniquely vulnerable position as a result of this crime, who will be supported on an individual basis
* Access to Medibank’s mental health and wellbeing support line for all customers, including ahm customers
* Access to specialist identity protection advice and resources from IDCARE
* Free identity monitoring services for customers who have had their primary ID compromised
* Reimbursement of fees for re-issue of identity documents that have been fully compromised in this crime

We will also defer premium increases for Medibank and ahm customers which were scheduled to rise on 1 November 2022, now to occur on 16 January 2023.

We have also established specialised teams to help our customers who receive scam threats.  Customers report any suspicious emails or texts to  [Scamwatch](https://www.scamwatch.gov.au/).

We are also working with all Australian banks and relevant government departments to help them take additional steps to increase monitoring of affected customers accounts.

Update at 8.30am, Tuesday 25 October

There has been a further development in Medibank’s cybercrime event.

It has become clear that the criminal has taken data that now includes Medibank customer data, in addition to that of ahm and international student customers.

We have received a series of additional files from the criminal. We have been able to determine that this includes:

* A copy of the file received last week containing 100 ahm policy records – including personal and health claims data
* A file of a further 1,000 ahm policy records – including personal and health claims data
* Files which contain some Medibank and additional ahm and international student customer data

Given the complexity of what we have received, it is too soon to determine the full extent of the customer data that has been stolen.

We will continue to analyse what we have received to understand the total number of customers impacted, and specifically which information has been stolen.

We will also continue to contact our customers as we are able to confirm whether their data has been compromised.

We will continue to provide you with regular, transparent updates.

Update at 11:20pm, Thursday 20 October

We wanted to update you on the latest development, which the Australian Federal Police is investigating as a crime.

Medibank has been contacted by a criminal claiming to have stolen data and who has provided a sample of records for 100 policies which we believe has come from our ahm health insurance and international student systems. This information includes:

* First names and surnames
* Addresses
* Dates of birth
* Medicare numbers
* Policy numbers
* Phone numbers
* Some claims data, including the location of where a customer received medical services and codes relating to their diagnoses and procedures.

The criminal also claims to have stolen other information, including data related to credit card security. This has not yet been verified by our investigations.

We’re working around the clock to understand what additional customer data has been affected and how this will impact them.

We are making direct contact with the affected customers to inform them of this latest development, and to provide support and guidance on what to do next. We expect the number of affected customers to grow as the event continues.

Medibank urges customers to remain vigilant, and encourages them to seek independent advice from trusted sources, including the Australian Cyber Security Centre at [**cyber.gov.au**](https://www.cyber.gov.au/)

As always, Medibank will never contact customers requesting passwords or other sensitive information.

Medibank is in discussions with government stakeholders about what else we can do to assist our customers in safeguarding their identities and health information, and we will be in touch with customers about those steps directly.

For more information please [**read our latest media release on the Newsroom.**](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-response)

Update at 5:30pm, Friday 21 October

We are extending the operating hours of our contact centre this weekend.

Our contact centre will be open:

9am – 4pm (AEDT) on Saturday 22 October

9am – 2pm (AEDT) on Sunday 23 October

If you have any enquiries, please contact [13 23 31](tel:132331).

Update at 11:20pm, Thursday 20 October

We wanted to update you on the latest development, which the Australian Federal Police is investigating as a crime.

Medibank has been contacted by a criminal claiming to have stolen data and who has provided a sample of records for 100 policies which we believe has come from our ahm health insurance and international student systems. This information includes:

* First names and surnames
* Addresses
* Dates of birth
* Medicare numbers
* Policy numbers
* Phone numbers
* Some claims data, including the location of where a customer received medical services and codes relating to their diagnoses and procedures.

The criminal also claims to have stolen other information, including data related to credit card security. This has not yet been verified by our investigations.

We’re working around the clock to understand what additional customer data has been affected and how this will impact them.

We are making direct contact with the affected customers to inform them of this latest development, and to provide support and guidance on what to do next. We expect the number of affected customers to grow as the event continues.

Medibank urges customers to remain vigilant, and encourages them to seek independent advice from trusted sources, including the Australian Cyber Security Centre at [**cyber.gov.au**](https://www.cyber.gov.au/)

As always, Medibank will never contact customers requesting passwords or other sensitive information.

Medibank is in discussions with government stakeholders about what else we can do to assist our customers in safeguarding their identities and health information, and we will be in touch with customers about those steps directly.

For more information please [**read our latest media release on the Newsroom.**](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-response)

Update at 7:05pm, Wednesday 19 October

We want to update you on a new development in relation to the current cyber event.   
  
Today we received messages from a group that wishes to negotiate regarding their alleged removal of customer data. Urgent work is underway to establish if the claim is true, although based on our ongoing forensic investigation we are treating the matter seriously at this time.    
  
Our systems have not been encrypted by ransomware, which means usual activities for customers continues. Our ongoing response to safeguard our networks and systems may cause necessary temporary disruptions to our services.    
  
We understand this news may cause you concern and we’re sorry. We will continue to keep you updated on this page as our investigations continue.

For more information please [**read our latest media release on the cyber event**](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-update-19-October).

Update at 5:40pm, Tuesday 18 October

We are pleased to confirm all systems are again operating for our ahm health insurance and international student customers. We apologise for the inconvenience this disruption has caused.

Update at 3:50pm, Tuesday 18 October

Our ahm health insurance and international student member services and policy management systems have been taken offline. This will cause disruptions for some of our customers. Customers will still be able to contact our customer teams via phone but at this stage our people won’t be able to access policy information. We apologise for the inconvenience this will cause some customers.

Our systems for other Medibank customers have remained uninterrupted at this time.

Update at 9:30am, Monday 17 October

An update from CEO David Koczkar:

"Our ongoing investigation continues to show no evidence that any customer data has been removed from our IT environment.

"We have resumed normal activity for our customers, after temporarily removing access to some of our customer systems as a precautionary measure last week.

"We’re sorry for the inconvenience and concern this may have caused.

"Our ongoing investigation has found the unusual activity we detected in part of our IT network was consistent with a possible ransomware threat. Ransomware is a common and dangerous type of malicious software that works by locking up or encrypting files, so they are no longer accessible. Our systems were not encrypted by ransomware during this event.

"As a further precaution, we’ve put in place additional security measures across our network and we continue to work with external cybersecurity experts and the Australian Government’s lead cyber agency, with our forensic investigation continuing.

"We remain vigilant and will take necessary steps in the future to protect your data. Although there is nothing that customers need to do, you can contact us by phone."

For more information please [**read our latest media release on the cyber event**](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-and-trading-update).

Update at 5:30pm, Friday 14 October

We are pleased to advise that our ahm health insurance and international student customers can now log in to their member accounts.

We apologise for the regrettable inconvenience this disruption has caused some customers.

Update at 2:15pm, Friday 14 October

As Medibank continues to take decisive action in response to the ongoing cyber event, temporary disruptions to services may occur.

Higher than usual customer traffic was causing some delays to ahm health insurance and international student customers logging in to their member accounts. We’ve temporarily restricted these services to ensure customers can continue to make claims and access their policies via our phone team.

We apologise for the regrettable inconvenience this will cause some customers.

Please bear with us as we continue working to safeguard our customers and people, and ensure that services are available to those who rely on us for their health and wellbeing.

While our investigation is continuing, at this stage we have found no evidence that our customer data has been accessed. We remain focused on taking all steps required to contain the event and ensure the ongoing security of our customers, our people and stakeholder information and the delivery of our services.

Update at 10:30am, Friday 14 October

A message from our CEO David Koczkar:

“I’m pleased to say our ahm and international students can now resume their normal activities after we restored access to our systems. I apologise for the disruption this has caused.

"Importantly, as we’ve continued to investigate all aspects of the event, we have still found no evidence that customer data has been accessed.

"As we continue to take decisive action to safeguard our networks and systems, we will take any steps necessary to protect the data of our customers, people and other stakeholders.

"As a health company providing health insurance and health services, we hold a range of necessary personal and private customer data. The protection of our customers and their data security is our highest priority.

"Our health services continue to be available to our customers, this includes their ability to access their health providers.

"We’ll continue to provide regular updates as we have more information.”

Update at 10:00am, Friday 14 October

Medibank Group has now restored access to our ahm health insurance and international student policy systems.

We are still responding to the cyber event that we alerted our customers, people, other stakeholders and the ASX about on Thursday.

A forensic investigation continues, and it will take time.

Update at 9:30am, Friday 14 October

Yesterday we began the process of communicating to our customers about the event with around 2.8 million emails now sent to Medibank and ahm health insurance customers (example pictured), and text messages are being sent to customers whose preferred communication method is text message.

We are in frequent contact with the Australian Cyber Security Centre, our regulators, government departments and other key stakeholders to keep them updated.

[View example email we have sent to our customers](https://www.medibank.com.au/content/dam/retail/cybersecurity/Medibank%20cyber%20incident%20communication.png)

Text

Description automatically generated

Update at 5:00pm, Thursday 13 October

We confirm we have successfully taken offline the ahm health insurance and international student policy systems and its data, and we are in the process of methodically and safely restarting the systems.

The work we have done today continues to show no evidence that customer data has been accessed, however our investigation is ongoing.

We have spoken with the Australian Cyber Security Centre, APRA, Office of the Australian Information Commissioner, Private Health Insurance Ombudsman, the Department of Health and the Department of Home Affairs over the course of the day to ensure that our regulators and other key stakeholders are informed.

We have begun the process of contacting our customers and our focus remains on ensuring the ongoing security of our customers, employees and stakeholders and the continued delivery of Medibank services. Our highest priority remains resolving this matter transparently and as quickly as possible.

Update at 11:00am, Thursday 13 October

Yesterday the Medibank Group detected unusual activity on its network.

In response to this event, Medibank took immediate steps to contain the event, and engaged specialised cyber security firms.

At this stage there is no evidence that any sensitive data, including customer data, has been accessed.

As part of our response to this event, Medibank will be isolating and removing access to some customer-facing systems to reduce the likelihood of damage to systems or data loss.

As a result our ahm health insurance and international student policy management systems have been taken offline. We expect these systems to be offline for most of the day.

This will cause regrettable disruptions for some of our customers. ahm health insurance and international student customers will still be able to contact our customer teams via phone but at this stage our people won’t be able to access policy information.