Medibank Private Limited and AHM Cyber Incident

On the 20 October 2022, Medibank Private Limited (Medibank Private) released a statement advising that it had been contacted by a criminal claiming to have stolen Medibank Private and AHM data. The data includes names and addresses, dates of birth, Medicare card numbers, policy numbers, phone numbers and some claims data.

Medibank Private advises that it has begun making direct contact with affected customers.

If you think you may be affected, **Medibank Private customers should contact 13 23 31 and AHM customers should contact 13 42 46**. For more information, see Medibank Cyber Incident.

You should also:

- Secure and monitor your devices and accounts for unusual activity, and ensure they have the latest security updates.
- Enable multi-factor authentication for all accounts.
- If you need assistance with taking these steps, please visit cyber.gov.au.

Be alert for scams referencing this incident. Learn how to protect yourself from scams by visiting Scamwatch.

If you are concerned that your identity has been compromised or you have been a victim of a scam, contact your bank immediately and call IDCARE on 1800 595 160.

If your identity has been stolen, you can apply for a Commonwealth Victims' Certificate.

If you believe you are victim of a cybercrime, report using ReportCyber at cyber.gov.au.

The following websites can help you protect yourself and stay informed:

- Identity theft | Moneysmart.
- Identity fraud | OAIC.
- cyber.gov.au.

If you wish to make a privacy complaint, please contact Medibank Private. If you are unable to resolve your complaint with Medibank Private, you may wish to lodge a complaint with the Office of the Australian Information Commissioner.

What is the Government doing to protect your identity?

The Australian Government understands the cyber incident within Medibank Private is very stressful for affected customers. The Government is working around the clock to make sure that people's information is protected and to minimise the impact of this incident.

Medibank Private is working closely with the Australian Signals Directorate’s Australian Cyber Security Centre (ACSC), the Office of the Australian Information Commissioner, the Australian Federal Police (AFP), and other government regulators.

The ACSC is supporting Medibank with cyber security incident response and ongoing technical advice.

The AFP has launched Operation Pallidus to investigate the incident.

The Department of Health and Aged Care has also been in contact with Medibank Private to understand the implications for privately insured consumers, and to understand and support Medibank Private’s strategy to communicate with affected customers.

If your Medicare card number has been exposed and you are concerned, you can replace your Medicare card for free. You can do this using your Medicare online account through myGov, the Express Plus Medicare mobile app, or calling the Medicare program.

Services Australia is putting in place additional security measures to protect your information. If you believe there has been unauthorised activity in your Medicare account, you can call the Services Australia Scams and Identity Theft Help Desk. They can help secure your account if it’s been compromised. For more information, go to servicesaustralia.gov.au.

The Government will continue to update this factsheet as more information becomes available.