Australian Government
Office of the Australian Information Commissioner

Medibank civil penalty action

Medibank data breach

Medibank and its subsidiary ahm experienced a cyber attack in 2022. One or more threat actors accessed and extracted personal information of millions of current and former customers.

The Australian Information Commissioner alleges the threat actor then published data on the dark web, including:

- names
- dates of birth
- gender
- Medicare numbers
- home addresses
- email addresses
- phone numbers
- visa details
- health claims data (including provider names, locations and contact details; diagnosis numbers; procedure numbers; and dates of treatment).

OAIC investigation

The OAIC commenced an investigation into Medibank's privacy practices following the data breach.

The investigation focused on how Medibank managed and secured personal information and whether the steps it took were reasonable in the circumstances to protect personal information from misuse, unauthorised access and/or disclosure.

Civil penalty action

The Australian Information Commissioner alleges Medibank seriously interfered with the privacy of 9.7 million Australians by failing to take reasonable steps to protect their personal information from misuse and unauthorised access or disclosure in breach of the *Privacy Act 1988*.

The Australian Information Commissioner considers Medibank did not take reasonable steps to protect personal information it held given its size, resources, the nature and volume of the sensitive and personal information it handled, and the risk of serious harm for an individual in the case of a breach.

Next steps

The case is before the Federal Court and is subject to the court's case management processes.

Penalties

The Federal Court can impose a civil penalty of up to $2.22 million for each contravention. The Australian Information Commissioner alleges one contravention per each of the 9.7 million individuals whose privacy Medibank seriously or repeatedly interfered with.

Whether a civil penalty order is made and the amount are matters before the court.

Increased civil penalties of up to $50 million came into effect in December 2022, though do not apply to this case as the alleged contraventions occurred from March 2021 to October 2022.

Considerations for organisations

Organisations with obligations under the Privacy Act must take reasonable steps to protect personal information from misuse, interference and loss, and unauthorised access, modification or disclosure.

What constitutes reasonable steps depends on circumstances such as the:

- nature of the organisation
- amount and sensitivity of the personal information held
- possible adverse consequences for an individual in the case of a breach.

Reasonable steps might include, among other things, strategies and measures related to governance, culture and training, cyber security, third party providers and data breach preparation and response.

The OAIC encourages organisations to:

- layer security controls to avoid a single point of failure
- implement multi-factor authentication
- enforce password management policies
- ensure users have appropriate levels of access to information assets depending on their role and responsibilities, and monitor and regularly review the number accounts with more permissions than ordinary users
- implement robust security monitoring processes and procedures to ensure incidents are detected and responded to in a timely manner
- ensure effective oversight of third-party providers, including ensuring they have robust information security capabilities
- regularly review practices and systems, including actively assessing critical and sensitive infrastructure, and act on areas for improvement in a timely manner
- appropriately resource privacy and cyber security.

For more information on securing personal information, see chapter 11 of the OAIC's Australian Privacy Principles guidelines and the Guide to securing personal information. The OAIC publishes regular statistics on data breaches to help organisations understand and better mitigate privacy risks.