Article Information

Authors: Craig Subocz, Jan David Hohmann
Service: Cyber Security, Privacy & Data Protection
Sector: IT & Telecommunications

How to take reasonable steps to protect personal information: Early learnings from the Information Commissioner's civil penalty enforcement action against Medibank Private Limited

On 17 June 2024, the Privacy Commissioner published a redacted version of the Concise Statement filed in the Federal Court of Australia for Medibank Private's alleged breaches of Australian Privacy Principle (APP) 11 arising out of the data breach that affected the information of millions of Australians. While the proceedings have only just begun, the Concise Statement nonetheless sets the benchmark for the reasonable steps the Commissioner expects organisations dealing with sensitive information to implement.

Background

In October 2022, Medibank Private Limited (**Medibank**) suffered a significant data breach that exposed the personal and sensitive information of millions of its customers. In June 2024, the Australian Information Commissioner commenced civil penalty proceedings under the *Privacy Act* 1988 (Cth) (**Privacy Act**) against Medibank, alleging that 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.

On 17 June 2024, the Australian Information Commissioner published a redacted version of the Concise Statement filed with the Court. The purpose of the Concise Statement is to concisely set out the important facts of the claim, the relief sought (and from whom), the causes of action for the relief and the alleged harm suffered by the applicant.

The allegations against Medibank

The Concise Statement alleges that Medibank contravened APP 11.1, which requires entities bound by the *Privacy Act* to take reasonable steps to protect personal information they hold from misuse, interference, loss, and unauthorized access. Essentially, the Australian Information Commissioner alleges that Medibank failed to take reasonable steps to protect personal and sensitive information, and those alleged failures caused the data breach.

In particular, the Commissioner alleges that a contractor engaged by Medibank to provide IT support services saved his Medibank login credentials to his personal internet browser on one work computer and then "synced" those credentials to another computer used for personal purposes which was then compromised through malware, allowing the Medibank credentials to be stolen. The Commissioner further alleges that the threat actors used the login credentials to gain unauthorized access to Medibank's corporate network and steal 520 gigabytes of data, including the personal and sensitive information of Medibank customers.

The Commissioner alleges that Medibank permitted remote access without the need to complete multi-factor authentication. Additionally, the Commissioner alleges that while Medibank had implemented security systems with various automatic alerts triggered by the threat actor's activities, these alerts were not appropriately triaged or escalated by Medibank or its service provider, allowing the threat actor access to Medibank's corporate network for approximately six weeks.

The Commissioner further alleges that Medibank was aware of the shortcomings in its cyber security processes through a series of reports and audits it commissioned with external auditors, but Medibank failed to act promptly to address and

resolve the shortcomings.

Commissioner's expectations

It is important to note that, at the date of this insight, Medibank has not filed its defence to the Commissioner's claims and they are yet to be tested in court. Unless the matter is settled, it is likely that these claims will take significant time to be determined by a court.

However, relevantly for other organisations that collect and hold personal and sensitive information, the Concise Statement sets out a detailed description of the cyber security practices that the Commissioner alleges should have been implemented by Medibank in order to comply with the obligation imposed by APP 11 to take reasonable steps to protect the personal information Medibank held at the relevant time.

The Commissioner alleges that, having regard to the size, resources, the nature and volume of the personal information Medibank held, and the risk of harm to individuals in the case of a breach, Medibank should have implemented the following measures in order to satisfy its statutory obligation of taking reasonable steps to protect the personal information it held at the relevant time:

- Implement multi-factor authentication for authenticating remote access users to its corporate network and to authenticate users to sensitive or critical information assets once those users are within the Medibank network.
- Establish robust change management controls for information security configurations.
- Enforce strict privileged access management, limiting access to information based on user roles and responsibilities.
- Monitor privileged account activities closely and set alerts for suspicious behaviour.
- Enforce strong password complexity policies and prevent password reuse.
- Ensure encrypted storage of and audit of password usage for accessing critical data.
- Implement security monitoring to promptly detect and respond to incidents.
- Conduct regular security assurance testing, including penetration testing and internal audits.
- Strengthen application controls for servers hosting sensitive or critical information assets.
- Verify third party compliance with Medibank's information security policies and controls.

The Commissioner noted that the reasonableness of these measures was informed by various information and cyber security standards and frameworks, including the Essential Eight controls from the Australian Cyber Security Centre, Prudential Standard CPS 234, the Australian Signal Directorate's Information Security Manual and the ISO 27000 series of information security standards.

Serious interferences with the privacy of individuals

The Commissioner set out its preferred approach to the interpretation of the civil penalty provisions in the *Privacy Act*, which are found in section 13G of the *Act*. Noting that the legislation has now been amended to increase the civil penalties, the Commissioner claims that Medibank's alleged interferences with the privacy of individuals were "serious" for three reasons:

- The claimed shortcomings in Medibank's information security framework, including its alleged failure to implement basic security controls, having regard to the nature of the organization and the sensitive nature of the information it held;
- The nature of the personal information Medibank held; and
- The consequences of the data breach on affected individuals, including their exposure to harm, such as emotional distress, risk of identity theft, extortion and financial crime.

The Commissioner set out the preferred interpretation that Medibank contravened section 13G of the *Privacy Act* for each of the approximately 9.7 million individuals affected by the data breach. If the court accepts the Commissioner's interpretation and the claims against Medibank are sustained, then the maximum penalty for which Medibank could be liable would be astronomically high.

The Government has subsequently amended the *Privacy Act* to increase the penalties a court might apply for serious or repeated interferences with the privacy of individuals, as discussed further in our insight.

Conclusion

The list of actions the Commissioner alleges Medibank should have taken but did not is based on the particular circumstances of Medibank and the information it collects and holds. Not every organisation will be in a similar position to Medibank. However, the Concise Statement sets out a useful checklist of measures each organisation should consider

implementing in order to demonstrate compliance with their statutory obligation to take reasonable steps to protect the personal information they collect and hold.

Therefore, your organisation should review their information security practices against the list of measures the Commissioner alleges should have been taken by Medibank, taking into account differences in the nature of the information held and the respective size of the organisation with Medibank. Particular importance should be paid to the cyber security and information security standards and frameworks that may be relevant to your organisation's industry and business.

However, simply using the Commissioner list as a checklist will not necessarily suffice. Due to the evolving cyber security landscape where security threats continuously evolve, care should be taken to ensure that your organisation continues to adapt and evolves its information security framework.