Baker McKenzie.

Client Alert

October 2025

Australia: A New Era of Enforcement - First Privacy Act Penalty Issued for Eligible Data Breach

Australian Information Commissioner v Australian Clinical Labs Limited (No 2) [2025] FCA 1224

In brief

The Federal Court has ordered Australian Clinical Labs Limited (ACL) to pay a $5.8 million civil penalty in connection with a data breach involving Medlab Pathology Pty Ltd (Medlab), which was acquired by ACL in December 2021. This is the first civil penalty proceeding brought by the Australian Information Commissioner (Commissioner) in the history of the Privacy Act 1988 (Cth) (Act).

The Court assessed the test for "reasonable steps" by organisations to protect personal information, and the delay by ACL in undertaking an eligible data breach assessment and issuing a notification to the Commissioner.

This case marks a shift towards stricter regulatory enforcement and highlights the need for organisations to be diligent in preventing and responding to eligible data breaches.

Contents

In depth

Background

Decision

Penalties

Takeaways

In depth

Background

A brief chronology of the incident is as follows:

- On 19 December 2021, ACL acquired the assets of Medlab, including all of Medlab's IT systems.
- On or before 25 February 2022 (the date of first awareness), Medlab experienced a cyberattack initiated by threat actor, the Quantum Group.
- On 21 March 2022, on advice from third party cybersecurity experts, StickmanCyber, ACL determined that there had not been an "eligible data breach", as defined by s 26WE of the Act. ACL assessed that notification to the Commissioner or individuals of the data breach was therefore not required. ACL did not receive external legal advice on this point. At that time, ACL did not believe that any data had been exfiltrated from the IT systems.
- On or before 16 June 2022, the Quantum Group published 86 gigabytes of data exfiltrated from Medlab's IT systems (which were ultimately owned by ACL), including the personal and sensitive health information of more than 223,000 individuals, on the dark web. On the same date, ACL validated the exfiltration and publication of Medlab's data and internally assessed that an eligible data breach had likely occurred.
- On 10 July 2022, following a review of the exfiltrated and published data, ACL notified the Commissioner that it had reasonable grounds to believe that an eligible data breach had occurred. Notifications to affected individuals were issued after this date.

Decision

The Court ultimately found, as agreed between the parties, that ACL had committed a serious interference with privacy in contravention of s 13G(a) of the Act by reason of breach of:

- Australian Privacy Principle (**APP**) 11.1(b), which requires organisations to take reasonable steps to protect personal information it holds from unauthorised access, modification or disclosure;
- s 26WH(2) of the Act, which requires organisations to carry out a reasonable and expeditious assessment of a suspected data breach; and
- s 26WK(2) of the Act, which requires organisations to notify the Commissioner as soon as practicable after making an assessment that there are reasonable grounds to believe that there has been an eligible data breach.

Breach of APP 11.1(b)

ACL was found to have breached APP 11.1(b) on the basis that it had inadequate cybersecurity controls in place and therefore had not taken steps that were *"reasonable in the circumstances"* to protect the personal information that it held from unauthorised access, modification or disclosure.

The Court noted that APP 11.1(b) had not been the subject of any previous judicial consideration, applied an objective standard when applying APP 11.1(b), and suggested that the circumstances can be considered broadly. The Court stated that the relevant circumstances could include:

- the sensitivity of the information;
- the possible harm caused to individuals if the information is released;
- the size of the APP entity (meaning an agency or organisation subject to the Act as set out in s 6(1) of the Act);
- the cybersecurity risks in the context of the industry that the APP entity operates in; and
- whether there have been any previous cyberattacks or threats made against the APP entity.

In its assessment of reasonableness, the Court considered other legislation that imports a "*reasonable steps"* obligation. The Court ultimately assessed that reasonable steps should be assessed objectively on a case-by-case basis, could not simply be delegated, and require a wholistic analysis of the organisation.

The Court considered the threshold for "s*eriousness"* of the contravention under s 13G(a) of the Act of the Act had been met, having regard to the nature and volume of the personal information (including sensitive health information), the extent of Medlab's cybersecurity deficiencies, and ACL's reliance on a third party cybersecurity services provider.

More specifically, the Court found that ACL's ability to detect and respond by itself to cyber incidents was deficient because:

- the ACL cyber incidents playbooks did not clearly define roles and responsibilities for incident response efforts, contained limited detail on containment processes that should be deployed in the event of a cyber incident or steps that ACL should take to mitigate exfiltration of data in the event of a cyber incident, and recommended steps for technologies that were not used within the Medlab IT systems;
- there was inadequate testing of incident management processes in the period between the acquisition of the Medlab IT systems and the data breach;
- Data Loss Prevention was not used on the Medlab IT systems to detect or prevent the theft of personal information and data held on those systems;
- adequate tooling/products that could perform behavioural-based analysis of activities in order to determine whether malicious actions might be undetected by an antivirus product were not used;
- there was no application whitelisting in place to prevent unknown or unauthorised applications from running on Medlab computers;

there were only limited communications plans;

- the Medlab IT Team Leader had not seen, used, or received training on the playbooks provided and had no formal cybersecurity background or incident response training;

- there was limited security monitoring capability because the firewall logs were only retained for one hour;
- specific data recovery plans had not been developed; and
- Medlab staff were not required to use multifactor identification to use the Medlab VPN.

It is likely that the above list of deficiencies will be referred to by the Courts in the event of future legal action relating to cybersecurity and data breach incidents. As a result, organisations should consider closely their position on each of these elements.

Contravention of s 26WH(2)

ACL's third party cybersecurity services provider produced an incident summary report on 2 March 2022. The Court assessed that, by that date, ACL had subjective knowledge or awareness of circumstances that would give rise to a reasonable suspicion of an eligible data breach, such that an obligation to carry out a reasonable and expeditious eligible data breach assessment had arisen. ACL was required to take all reasonable steps to complete this assessment within 30 days.

ACL was found to have failed to undertake such an assessment due to its reliance on the inadequate assessment undertaken by its cybersecurity provider, knowing that the assessment was limited in scope and therefore not reasonable to rely upon. The Court further assessed that the failure to complete the stipulated reasonable and expeditious assessment likely resulted in a delay in notification to the Commissioner, which impeded the Commissioner's ability to perform her statutory function of monitoring ACL's notification to individuals whose personal information may have been compromised.

Contravention of s 26WK(2)

The Court found ACL to have contravened s 26WK(2) of the Act on the basis that it had failed to notify the Commissioner as soon as practicable after becoming aware of reasonable grounds to believe that an eligible data breach had occurred.

The Court was of the view that complying with s 26WK(2) is not particularly onerous, such that ACL could have provided notice to the Commissioner within two to three days of becoming aware of the reasonable grounds that there had been an eligible data breach. The Court assessed that date to be 16 June 2022, the date on which ACL became aware that information had been published on the dark web. Instead, ACL waited over 20 days to notify the Commissioner. The Court again noted that this delay impeded the Commissioner's ability to perform her statutory function regarding notification to affected individuals.

Penalties

Pursuant to its agreement with the Commissioner, ACL was ordered to pay the following amounts in relation to its contraventions of s 13G(a) of the Act:

- $4,200,000 with respect to its failure to take reasonable steps to protect the personal information it holds (where the maximum penalty was $495,060,000,000);
- $800,000 with respect to its delay in completing an eligible data breach assessment (where the maximum penalty was $2,200,000); and
- $800,000 with respect to its delay in notifying the Commissioner of an eligible data breach (where the maximum penalty was $2,200,000).

ACL was additionally ordered to pay $400,000 towards the Commissioner's costs.

The Court assessed the penalty as being appropriate by weighing six aggravating factors, such as how extensive the breaches were and ACL's failure to manage cybersecurity risks, against eight mitigating factors, which included there being no financial benefit to ACL and ACL's compliance history, ACL's co-operation with the Commissioner's investigation, the apology issued by way of ACL's ASX announcement, and, most importantly having regard to the potential maximum penalty of nearly $500 billion, that the contraventions arose from a single course of conduct.

Takeaways

1. This decision is a timely reminder that organisations should ensure that they:
    a. undertake adequate due diligence prior to and after acquiring another organisation's IT systems. Notably in this instance the incident occurred only approximately three months after ACL's acquisition of Medlab; and
    b. do not solely rely on third parties (e.g. cyber security providers and legal advisors), but rather have sufficient internal cyber incident detection mechanisms, which includes defined responsibilities for incident response and incident management processes.
2. The Court is not afraid to issue significant penalties for delay in conducting an eligible data breach assessment and/or issuing a notification to the Commissioner, especially if the delay is seen as impeding on the Commissioner's functions. In assessing a reasonable time to conduct an eligible data breach assessment, the Court did not refer to a specific timeframe, but examined when ACL had subjective knowledge or awareness of circumstances that were objectively sufficient to establish in the mind of a reasonable person a suspicion that an eligible data breach had occurred. This is notwithstanding the 30 day window set out in the legislation. An appropriate timeframe for notifying the Commissioner was assessed by the Court to be two to three days.
3. The aggregate civil penalty ordered by the Court was consented to by ACL. New penalty provisions have been introduced since this data breach occurred. Accordingly, it remains to be seen how the Court would decide on an appropriate civil penalty in circumstances where a penalty has not been agreed or under the new penalty regime.
4. It is important to understand the expectations of the Commissioner and Courts with respect to reasonable preventative measures and incident response processes in the particular context of an organisation's size, industry, and unique circumstances.
5. Although notifications to affected individuals were not considered in this decision, organisations must be prepared to commence issuing notifications to affected individuals as soon as practicable after completing an eligible data breach assessment, and particularly at the time of notification to the Commissioner.

Link to the case is **here**

Contact Us

Paul Forbes
Partner
Paul.Forbes@bakermckenzie.com

Ryan Grant
Partner
Ryan.Grant@bakermckenzie.com

Adrian Lawrence
Partner
Adrian.Lawrence@bakermckenzie.com

Anne Petterd
Partner
Anne.Petterd@bakermckenzie.com

Caitlin Whale
Partner
Caitlin.Whale@bakermckenzie.com

Jarrod Bayliss-McCulloch
Special Counsel
Jarrod.Bayliss-McCulloch@bakermckenzie.com

Simone Blackadder
Special Counsel
Simone.Blackadder@bakermckenzie.com

Hannah Stacey
Associate
Hannah.Stacey@bakermckenzie.com