Take another look at privacy risk: Australia's first civil penalty may help you quantify it!

On 8 October 2025, the Office of the Australian Information Commissioner (**OAIC**) secured civil penalties under the Privacy Act 1988 (Cth) (**Act**) against Australian Clinical Labs Limited (**ACL**).[1] This concludes almost 2 years of Federal Court proceedings[2] and negotiations resulting in a AUD$5.8m settlement and AUD$400,000 contribution towards OAIC's costs.

These sums could be seen as modest, representing less than 0.9% of ACLs annual revenue and less than 0.0012% of the half a trillion (AUD$495,060,000,000) statutory penalty limit [calculated as 2,000 penalty units[3] x 5(multiplier)[4] x AUD$222(cost per unit)[5] x 223,000(affected individuals)]. However, upon traversing the convoluted provisions of the Act and relevant case law, the Federal Court assessing the appropriateness[6] of the sum determined that it "*falls within the permissible range of penalties that would be sufficient for the purposes of both specific and general deterrence given the serious nature of the contraventions by ACL*".

ACL was ordered to pay the Commonwealth of Australia the sums of $4.2m, $800,000 and $800,000 respectively on account of 223,000 contraventions of APP11.1(b) (information security) and one breach respectively of sections 26WH(2) (breach assessment duty) and 26WK(2) (breach notification duty) of the Act. But the big news here really is that "*This is the first civil penalty proceeding brought by the Commissioner in the history of the Act*".

This case is preceded by the OAIC's landmark $50m settlement with Meta in December 2024[7] and the filing of civil penalty proceedings against Singtel Optus Pty Limited in August 2025. This growing regulatory and litigation risk will no doubt inspire boards, directors, investors and technology service providers across Australia to take a closer look at data privacy compliance.

Background

With the acquisition of Medlab Pathology Pty Limited on 19 December 2021, ACL became one of the largest private hospital pathology businesses in Australia, holding large volumes of sensitive information including prenatal genetic tests, fertility assessments and STD tests as well as patient financial information for invoicing.

Unfortunately, ACL failed to identify and mitigate Medlab's information security deficiencies, some of which were not investigated in due diligence. Even when discovered during integration, months went by operating with a lightweight antivirus, weak user authentication, inadequate firewalls, no file encryption, unsupported server OS, no data loss prevention, no MFA for VPN use, no behavioural-based monitoring and logging, no application whitelisting to prevent unknown apps, and no IT personnel training. This

[1] Australian Information Commissioner v Australian Clinical Labs Limited (No 2) [2025] FCA 1224 (link).
[2] Proceedings NSD1287/2023 filed on 2 November 2023.
[3] Section 13G set a limit of 2,000 penalty units in respect of each contravention at the relevant time in early 2022. In October 2025, the limit per contravention is the greater of AUD$50,000,000 or 3x the benefit or 30% of the adjusted turnover.
[4] Section 82(5) of Regulatory Powers (Standard Provisions) Act 2014 Cth sets the maximum penalty for corporates at 5x the limit. In October 2025, this multiplier still applies.
[5] The value of each penalty unit under section 4AA of the *Crimes Act 1914* (Cth). In October 2025, that value is $330.
[6] Section 82 of Regulatory Powers (Standard Provisions) Act 2014 (Cth).
[7] Enforceable undertakings from Meta Platforms, Inc. (Meta) to settle civil penalty proceedings in respect of Australian Facebook users impacted by the Cambridge Analytica matter, representing the largest ever payment dedicated to addressing concerns about the privacy of individuals in Australia (link).

was exacerbated by the high volume of sensitive information held by the well-resourced company, delays in risk assessments, overreliance on an external cybersecurity services provider and a lack of adequate procedures and skills to independently detect and respond to cyber incidents.

Information security under APP 11.1

Another first was that "*APP 11.1(b) has not been the subject of any previous judicial consideration.*" The Federal Court held that ACL failed to comply with the APP.

It analysed the scope of the "*circumstances*" to be taken into account when determining what sufficient "*reasonable steps*" to comply with APP11.1(b) might look like. The "*circumstances*" can be interpreted broadly and might include the data sensitivity, potential harm to individuals, entity sophistication, relevant cybersecurity environment and historic threats. The "*reasonable steps*" must be assessed objectively as expected of a reasonable person in a regulated position by looking at the totality of all systems, policies and procedures in place. The steps cannot be simply delegated. They will depend on the complexity of the business but do not equate to "*all reasonable steps*" and need not be "*optimal*".

The endless list of ACL's shortcomings included no incident response plan with defined roles and responsibilities, no detail about containment and mitigation steps, no adequate incident management rehearsals, limited communications plans and no data recovery plans.

The Federal Court was satisfied that the breaches of privacy of individuals were "*serious*" in the circumstances. Although not defined in the Act, according to case law, this question of fact depended on the breach being "*weighty, important, grave and considerable*".

"Eligible data breach"

Medlab suffered a ransomware attack by the Quantum Group on around 25 February 2022.

When the ransom demand was made, Medlab's external cybersecurity services provider reassured Medlab that "*…I don't feel that this will happen and it is merely a scare tactic, however, to err on the side of caution I would suggest that you prepare a statement stating that there was a malware incident but no data has been exfiltrated nor lost and the incident is being controlled…*".

Various "*limited*" investigations followed, somehow leading ACL to conclude in March 2022 that there was no "*eligible data breach*". Under the Act, an "*eligible data breach*" occurs if there is unauthorised access or disclosure of personal information which a reasonable person would conclude likely results in serious harm to any individual. The conclusion was reached despite ACL's knowledge of malicious code being installed on its network, an absence of logging and monitoring tools and warnings from the Australian Cyber Security Centre.

Around 16 June 2022, 86GB of exfiltrated data including health data and financial information relating to more than 223,000 Australian patients was published on the dark web. Between 22 June and 10 July 2022 Clyde & Co conducted an initial review of the data. ACL finally notified the OAIC on 10 July 2022.

Assessment of data breach

Whenever there are reasonable grounds to suspect a breach, the organisation must within 30 days carry out a reasonable and expeditious assessment to establish whether there are reasonable grounds to suspect that the circumstances amount to an eligible data breach.[8]

Despite Medlab's external cybersecurity provider's advice to the contrary, the Federal Court accepted that there were objectively sufficient circumstances to give rise to the requisite state of suspicion in the mind of a reasonable person that there may have been unauthorised access which would be likely to result in serious harm to individuals.

The external cybersecurity provider's report was inadequate as it related to limited hardware, only one firewall log, limited investigation of persistence mechanism installed by Quantum and no analysis of how Quantum operates or the likelihood of data exfiltration. In these circumstances, it was unreasonable for ACL to rely on the report.

Data breach notification

Under section 26 WK(2), the organisation must prepare and provide a statement to the OAIC that sets out certain mandatory information about the eligible data breach as soon as practicable after the data breach arising. The Federal Court held that ACL had reasonable grounds to believe that there had been an eligible data breach by at least 16 June 2022.

ACL failed to comply given that no notification had been provided to the OAIC until 10 July 2022, beyond any delay excusable by impracticability, e.g. prohibitive time, effort or cost in the circumstances. It is readily apparent that the OAIC breach notification form is not particularly onerous to complete and designed to easily provide the notification "*as soon as practicable*".

Civil penalties

Civil penalties are awarded at the Federal Court's discretion[9] on the OAIC's application.[10] That discretion must be exercised judicially and proportionately, balancing the public interest in promoting compliance, deterrence and any penalty's oppressive severity, recognising that the penalty quantum is fixed by "*instinctive synthesis*" of conflicting and contrasting considerations. A penalty must exceed any acceptable "*cost of doing business*" but not unfairly multiply liability for numerous contraventions arising from a single conduct.

When setting a penalty, predictability of outcomes should be ensured by considering all relevant aggravating and mitigating factors.[11] The Federal Court was persuaded that the penalty agreed between ACL and the OAIC was appropriate in all the circumstances, given the nature, extent, duration of the contraventions, the lack of care and due diligence, the hard to quantify but likely significant harm to individuals including financial harm, distress, psychological harm and material inconvenience, impact on public trust in organisations and their capability to promptly report breaches to allow the OAIC to act and enable individuals to protect themselves, and ACL's significant revenues of $995.6 million and net profit of $178.2 million in the financial year ending 30 June 2022.

[8] Section 26 WH(2) Privacy Act 1988 (Cth).
[9] Section 82 Regulatory Powers (Standard Provisions) Act 2014 (Cth)
[10] Section 80U Privacy Act 1988 (Cth)
[11] Section 82(6) Regulatory Powers (Standard Provisions) Act 2014 (Cth) and so-called "French factors" enunciated by French J in Trade Practices Commission v CSR Limited [1990] FCA 521.

Reviewing it through a different lens, the Federal Court accepted that $5.8 million could seem manifestly inadequate or outside of the permitted range to achieve deterrence, given the circumstances of the breach and the statutory maximum penalty of half a trillion AUD$. However, further mitigating factors such as ACL's negligence rather than wilfulness, cooperation and admissions, compliance programme, public apology and others led the Federal Court to conclude that, on the totality of facts and avoiding any oppressively severe penalty, an aggregate penalty of $5.8 million falls within the range of permissible penalties to achieve both specific and general deterrence. Concluding that this amount could not objectively be characterised as "*a cost of doing business*", it is sufficient as a deterrent signal to the healthcare system as a first historic shot by the OAIC.

What's next?

The Federal Court was happy to make the agreed declarations of contraventions to "*… provide a public indication of the seriousness with which the Court views the contraventions by ACL … , vindicate the Commissioner's claims that the conduct of ACL was unsatisfactory, and deter other APP entities from contravening the Act*".

The ACL penalty is being awarded under the old regime reserved for "*serious and repeated*" breaches and penalties capped at 2,000 units per contravention.[12] However, following the recent reform,[13] the OAIC will have an easier job establishing technical and non-serious breaches that can attract penalties of up to AUD$66k and AUD$660k, respectively. "*Serious*" breaches will attract the greater of AUD $50 million or 3x the value of any benefit obtained or 30% of the company's adjusted turnover per every single contravention. Corporate offenders will remain subject to a 5x multiplier.

There is an entire pipeline of OAIC's cases that will soon see the light of day. The ACL case highlights conduct which can be seen as a mitigating factor. Organisations under investigation should consider the benefits of conforming to such conduct if it is not too late.

Other lessons from the ACL case include:

- Corporate due diligence without a privacy and cyber assessment is rather risky.
- Questionnaire responses in due diligence must be supplemented with an independent vulnerability scan and penetration test.
- Cyber security is not just technical work. The case highlights that lawyers have a role to play in guiding organisations on how to comply with standards, advise on appropriate processes, flag gaps in reports, assess risk in crisis scenarios, and offering a firm voice interpreting legal requirements without undue regard to supposed practical constraints.
- Relying on an outsourced cybersecurity contractor alone may not be enough for compliance with the law or dealing with data breaches.
- Operating under identified and preventable risk is not acceptable.
- A good old "data map" might be needed to identify and mitigate risks in respect of all personal information held by the organisation.
- A lack of monitoring and logging tools will likely point to non-compliance.
- Incident response plans must be specific and living documents, ideally including a list of people with assigned responsibilities.

[12] Old wording of section 13G Privacy Act 1988 (Cth).
[13] The Privacy and Other Legislation Amendment Act 2024 (Cth).

- Without staff training, a policy or process will likely be worthless in mitigating legal risk.
- An active project seeking to improve data privacy and cyber compliance and establish a corporate culture of compliance will likely be viewed favourably when determining the amount of civil penalty.

Alexander Dittel is a Principal in **Data Privacy, Cyber and Digital** at KHQ Lawyers