FEDERAL COURT OF AUSTRALIA

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

File number(s):	NSD 1287 of 2023
Judgment of:	**HALLEY J**
Date of judgment:	8 October 2025
Catchwords:	**PRIVACY ACT** – Where an APP entity breached Australian Privacy Principle (**APP**) 11.1 of the *Privacy Act 1988* (Cth) (**Act**) by failing to take reasonable steps to protect personal information from unauthorised access or disclosure – what constitutes "reasonable steps" – where an APP entity interfered with the privacy of 223,000 individuals under s 13(1) of the Act by breaching an APP – where breaches of privacy constituted "serious contravention" under s 13G of the Act – where breach of privacy of each individual constituted a separate contravention of s 13G of the Act – where an APP entity was aware that there were reasonable grounds to suspect that there may have been an eligible data breach – where an APP entity failed to carry out a reasonable and expeditious assessment to determine whether there were reasonable grounds to believe that there was an eligible data breach in contravention of s 26WH of the Act – where contravention of s 26WH of the Act was serious – where an APP entity was aware that there were reasonable grounds to believe that there had been an eligible data breach – where an APP entity failed to prepare a statement in relation to the eligible data breach and provide it to the Commissioner in contravention of s 26WK of the Act – where contravention of s 26WK of the Act was serious – where a penalty was agreed between the regulator and the contravener –where a contravener admitted contraventions – where contraventions were extensive and significant – where it is not possible to quantify the loss or damage caused by contravening conduct – where contraventions were not deliberate – where a contravener cooperated with the regulator – where a contravener took meaningful steps to develop a satisfactory culture of compliance – where 223,000 contraventions arose from a single course of conduct – where the Court satisfied that agreed penalty falls within permissible range of penalties sufficient for both specific and general deterrence

Legislation:	*Australian Securities and Investments Act 2001* (Cth) *Corporations Act 2001* (Cth) ss 961L, 963F and 994E(5) *Crimes Act 1914* (Cth) s 4AA *Federal Court of Australia Act 1976* (Cth) s 21 *Privacy Act 1988* (Cth) ss 2A, 6, 6A, 6C, 13, 14, 15, 13G, 26WE, 26WF, 26WG, 26WH, 26WK, 26WL, 80U, Sch 1 *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth)
Cases cited:	*Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564 *Australian Building and Construction Commissioner v Pattinson* (2022) 274 CLR 450; [2022] HCA 13 *Australian Competition and Consumer Commission v Colgate-Palmolive Pty Ltd (No 3)* [2016] FCA 676 *Australian Competition and Consumer Commission v MSY Technology Pty Ltd* (2012) 201 FCR 378; [2012] FCAFC 56 *Australian Competition and Consumer Commission v Reckitt Benckiser (Australia) Pty Ltd* [2016] FCAFC 181 *Australian Competition and Consumer Commission v TPG Internet Pty Ltd* (2013) 250 CLR 640; [2013] HCA 54 *Australian Competition and Consumer Commission v Yazaki Corporation* (2018) 262 FCR 243, [2018] FCAFC 73 *Australian Securities and Investments Commission v Chemeq Ltd* [2006] FCA 936 *Australian Securities and Investments Commission v Diversa Trustees Limited* [2023] FCA 1267 *Australian Securities and Investments Commission v Firstmac Limited* [2024] FCA 737 *Australian Securities and Investments Commission v GetSwift Ltd (Penalty Hearing)* (2023) [2023] FCA 100; 167 ACSR 178 *Australian Securities and Investments Commission v Healey* (2011) 196 FCR 291; [2011] FCA 717 *Australian Securities and Investments Commission v Macquarie Bank Limited* [2024] FCA 416 *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151; (2021) 172 ACSR 1 *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (No 2)* [2021] FCA 877; (2021) 156 ACSR 371

	Australian Securities and Investments Commission v Rich [2004] NSWSC 836; (2004) 50 ACSR 500 *Australian Securities and Investments Commission v Westpac Banking Corporation (No 3)* [2018] FCA 1701 *Clarke (as trustee of the Clarke Family Trust) & Ors v Great Southern Finance Pty Ltd (Receivers and Managers Appointed) (in liquidation) & Ors* [2014] VSC 516 *Commonwealth v Director, Fair Work Building Industry Inspectorate* (2015) 258 CLR 482; [2015] HCA 46 *Forster v Jododex Australia Pty Ltd* (1972) 127 CLR 421 *Provide Nominees Pty Ltd v Australian Securities and Investments Commission* [2024] FCA 303 *Rural Press Ltd v Australian Competition and Consumer Commission* (2003) 216 CLR 53; [2003] HCA 75 *Trade Practices Commission v CSR Limited* [1990] FCA 521 *Vines v Australian Securities and Investments Commission* [2007] NSWCA 126; (2007) 63 ACSR 505 *Volkswagen Aktiengesellschaft v Australian Competition and Consumer Commission* (2021) 284 FCR 24; [2021] FCAFC 49
Division:	General Division
Registry:	New South Wales
National Practice Area:	Commercial and Corporations
Sub-area:	Regulator and Consumer Protection
Number of paragraphs:	141
Date of hearing:	29 September 2025
Counsel for the Applicant:	Dr R C A Higgins SC with Ms E Bathurst
Solicitor for the Applicant:	DLA Piper
Counsel for the Respondent:	Ms Z Hillman
Solicitor for the Respondent:	Gilbert + Tobin

ORDERS

NSD 1287 of 2023

BETWEEN:	**AUSTRALIAN INFORMATION COMMISSIONER** Applicant
AND:	**AUSTRALIAN CLINICAL LABS LIMITED (ACN 645 711 128)** Respondent

ORDER MADE BY: **HALLEY J**

DATE OF ORDER: **8 OCTOBER 2025**

THE COURT DECLARES THAT:

Breach of APP 11.1 – failure to take reasonable steps to protect personal information

1. In contravention of s 13G(a) of the *Privacy Act 1988* (Cth) (**Privacy Act**), in the period between 19 December 2021 and 15 July 2022, the respondent (**ACL**) engaged in a practice that was an interference with the privacy of one or more individuals because, having acquired the assets of Medlab Pathology Pty Limited (**Medlab**) on 19 December 2021, ACL did not have in place adequate cybersecurity controls, which meant that it did not take reasonable steps to protect the personal information of those individuals that ACL held on certain Medlab servers from unauthorised access, modification or disclosure, in contravention of Australian Privacy Principle 11.1(b) (**Personal Information Contraventions**).

Contravention of s 26WH(2) – failure to carry out a reasonable and expeditious assessment

2. In contravention of s 13G(a) of the Privacy Act, within 30 days of 2 March 2022, in circumstances where in or around February 2022, the computer systems ACL had acquired from Medlab in December 2021 were the subject of a cyberattack (**Medlab Cyberattack**), ACL failed to take reasonable steps to ensure it carried out a reasonable and expeditious assessment of whether there were reasonable grounds to believe that the circumstances of the Medlab Cyberattack amounted to an eligible data breach within the meaning of s 26WE of the Privacy Act, in contravention of s 26WH(2) of the Privacy Act (**Assessment Contravention**).

Contravention of s 26WK(2) – failure to notify of data breach

3. In contravention of section 13G(a) of the Privacy Act, having formed the view by at least 16 June 2022 that there were reasonable grounds to believe that there had been an eligible data breach in the circumstances of the Medlab Cyberattack, ACL failed to prepare and give to the Australian Information Commissioner (**Commissioner**), as soon as practicable, a statement concerning the Medlab Cyberattack outlining the matters set out in section 26WK(3) of the Privacy Act, in contravention of s 26WK(2) of the Privacy Act (**Notification Contravention**).

THE COURT ORDERS THAT:

4. ACL is to pay to the Commonwealth of Australia, within 30 days, a civil penalty of $5,800,000, comprised of:

   (a) $4,200,000 in respect of the Personal Information Contraventions;

   (b) $800,000 in respect of the Assessment Contravention; and

   (c) $800,000 in respect of the Notification Contravention.

5. ACL is to pay to the Commissioner, within 30 days, a contribution of $400,000 towards the Commissioner's costs in the proceeding.

6. The proceeding otherwise be dismissed.

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

REASONS FOR JUDGMENT

HALLEY J:

A. INTRODUCTION

1 The respondent, Australian Clinical Labs Limited (**ACL**), is and was during the period from 19 December 2021 to 15 July 2022 (**Relevant Period**), one of the largest private hospital pathology businesses in Australia. In the course of the conduct of its business as a provider of healthcare services, ACL collects and holds individual patient's personal and sensitive information, including health information, for the purposes of providing test results and issuing invoices.

2 On 19 December 2021, ACL acquired the assets of **Medlab** Pathology Pty Ltd. From the date of acquisition, ACL owned and controlled Medlab's computer and communications hardware, computer and information technology systems, equipment, and software (**Medlab IT Systems**).

3 On or shortly prior to 25 February 2022, the Quantum Group initiated a cyberattack against the Medlab IT Systems (**Medlab Cyberattack**).

4 The Medlab Cyberattack resulted in 86 gigabytes of data, including the personal and sensitive health information of more than 223,000 individuals, being exfiltrated and subsequently published on the dark web.

5 On 2 November 2023, the applicant, the Australian Information Commissioner (**Commissioner**), commenced this proceeding seeking declarations that ACL had contravened s 13G(a) of the *Privacy Act 1988* (Cth) (**Act**) by failing to (a) take reasonable steps to protect individuals' personal information that it held over the period from 26 May 2021 to 29 September 2022, in breach of Australian Privacy Principle (**APP**) 11.1(b), and (b) conduct a reasonable assessment of whether the Medlab Cyberattack constituted an "eligible data breach" (as this concept is defined in the Act) and then failing to notify the Commissioner as soon as practicable, in contravention of s 26WH(2) and s 26WK(2) of the Act.

6 This is the first civil penalty proceeding brought by the Commissioner in the history of the Act.

7 Although ACL consents to the making of the declarations and the imposition of the aggregate civil penalty sought by the Commissioner, it is necessary for the Court to determine whether the declarations and pecuniary penalty orders are appropriate and should be made. For the

following reasons, I have concluded that having regard to all the relevant circumstances the aggregate agreed penalty of $5,800,000 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.

B. AGREED FACTUAL BACKGROUND

Overview

8 The parties jointly relied on a statement of agreed facts and admissions (**SAFA**). A copy of that document which has been redacted to suppress information the subject of suppression orders made by the Court is attached to these reasons as Annexure A. The facts and admissions concern the Relevant Period.

9 For present purposes, it is sufficient to provide the following summary of the matters included in the SAFA that are relevant to ACL's contravening conduct.

ACL

10 ACL is and was during the Relevant Period, an APP entity within the meaning of the Act.

11 ACL employed approximately 5,400 staff as at 30 June 2022, and approximately 5,115 staff as at 30 June 2023.

12 ACL is and was during the Relevant Period one of the largest private hospital pathology businesses in Australia, generating revenue of: $674.4 million in the financial year ending June 2021, $995.6 million in the financial year ending June 2022, and $697.1 million in the financial year ending June 2023.

13 During the Relevant Period, ACL was operating in a high cyber threat landscape with a significant cyber risk profile and was aware of that fact.

ACL acquisition and integration of Medlab assets

14 On 19 December 2021, ACL acquired the assets of Medlab. Medlab was a privately owned pathology business which provided and/or facilitated the provision of health services in New South Wales and Queensland, including prenatal genetic testing, fertility assessments and testing for sexually transmitted diseases.

15 At the time of the acquisition, Medlab collected and held individuals' personal and sensitive information in the course of its business. This information included health information, contact

information, credit card information and payment details relating to more than 223,000 individuals.

16 ACL did not identify certain relevant vulnerabilities in the Medlab IT Systems prior to its acquisition of the Medlab assets.

17 In January 2022, ACL established a steering committee to oversee and coordinate the integration of the Medlab IT Systems into ACL's core IT environment by 30 June 2022, (or, if integration was not appropriate, decommission). The steering committee included ACL's Chief Information Officer (**CIO**), Chief Operating Officer, Chief Executive Officer (**CEO**), Chief Financial Officer and other State Executive Officers and general managers.

18 Until they were integrated into ACL's core IT environment, the Medlab IT Systems had cybersecurity deficiencies, including that (a) the antivirus software deployed by Medlab computers was not capable of preventing certain malicious files from being written or run on those systems, (b) Medlab computers utilised weak authentication measures, (c) they were subject to firewalls that could only log one hour of activity before the logs were deleted, (d) they had no form of file encryption, (e) the Medlab network server was running a legacy system of a Windows server that was not supported by Microsoft from 14 January 2020, and (f) the antivirus software deployed on the Medlab server did not prevent or detect a threat actor uploading data from the server to the internet (**Medlab IT Systems Deficiencies**).

Cyberattack by Quantum Group

19 On or before 25 February 2022, a threat actor, known as the Quantum Group, made the Medlab Cyberattack. It involved a ransomware demand from the Quantum Group which had accessed several of the Medlab IT Systems and installed malware on them.

20 ACL's initial response to the Medlab Cyberattack was dependent on a third-party cybersecurity services provider, StickmanCyber, which has been engaged by ACL since February 2021 to provide services in relation to ACL's IT environment more generally, including to conduct a review of ACL's cybersecurity processes and controls.

21 The Medlab IT Team Leader who was initially put in charge of the response had received no training in how to respond to a cyberattack, including in respect of the malware and outbreak playbook and ransomware playbook that she was given by ACL's Head of Technical Services once ACL became aware of the Medlab Cyberattack.

22 At around 1.32 pm on 25 February 2022, ACL instructed StickmanCyber to investigate, respond to, and provide advice in relation to the Medlab Cyberattack.

23 At 10:48 pm on 25 February 2022, StickmanCyber informed ACL that (relevantly) the Quantum Group's ransom note stated that in 48 hours, they will "post your data on site, ETC" but then stated:

> …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...

24 On 1 March 2022, StickmanCyber ceased investigating whether there had been any exfiltration of data as a result of the Medlab Cyberattack, with the last dark web scan being conducted on that day.

25 On 2 March 2022, StickmanCyber provided ACL with an "Incident Summary Report" (**Report**) summarising its findings and conclusions resulting from 44.5 hours of investigating the Medlab Cyberattack. In the Report, StickmanCyber stated that the "Root Cause" computer was infected, and "TSsel.exe was executed" by (a) spreading across the network, (b) adding "attribute .quantum" to all readable files, and (c) encrypting all .quantum files.

26 StickmanCyber conducted a limited investigation of whether the Quantum Group may have established mechanisms to stay connected to the Medlab IT Systems and its network.

27 On 11 March 2022, StickmanCyber closed its investigation.

28 On 15 March 2022, StickmanCyber sent an email to ACL's Head of Technical Services concerning the notifiable data breach scheme in the Act and provided a link to the website of the Office of the Commissioner. StickmanCyber concluded the email by stating that at the point they had ended their engagement, they "would have to say" that the Medlab Cyberattack did not cause harm to any individual.

29 By 18 March 2022, ACL's CIO and Head of Technical Services formed a view that the threat posed by the Medlab Cyberattack had been contained, and that there was no information suggesting that personal information held by the Medlab IT Systems had been exfiltrated.

30 By 21 March 2022, based on the analysis conducted and the advice provided by StickmanCyber, ACL had determined that the Medlab Cyberattack was not an eligible data breach within the meaning of s 26WE of the Act.

31 At 5.28 am on 25 March 2022, the Australian Cyber Security Centre (**ACSC**) notified ACL that it had received intelligence from a trusted third party that Medlab may have been a victim of a ransomware incident and reminded ACL that it may be required to notify the Commissioner and affected individuals (**first ACSC notification**).

32 At 3.10 pm on 25 March 2022, ACL's CIO sent an email to the ACSC with details of the Medlab Cyberattack and informed the ACSC that, following monitoring of impacted devices and the dark web, ACL did not believe that any data had been exfiltrated.

33 On 29 March 2022, ACL's CIO advised the ACL board that:

> … no exfiltration of data was detected out of the network. At this point we have no reason to believe any [personal health information] or company data was breached…

Publication of exfiltrated data on the dark web

34 On or before 16 June 2022, 86 gigabytes of data exfiltrated by the Quantum Group from the Medlab IT Systems was published on the dark web. At least some of the exfiltrated data comprised personal information and sensitive information for the purposes of s 6 of the Act.

35 At 10.26 am on 16 June 2022, the ACSC sent ACL a second notification (**second ACSC notification**), which included the following statements:

> …it has come to our attention that potentially 80gb of Medlab data was published from the Quantum group. Initial investigation by the third party has shown that Personal Identifiable Information (PII), Protected Health Information (PHI), and financial information is available …

36 At 2.53 pm on 16 June 2022, ACL's Head Of Technical Services sent an email to individuals at ACL, Medlab and StickmanCyber stating that he was satisfied that data containing complete credit card information and personal information had been exfiltrated during the Medlab Cyberattack, was publicly visible on the dark web, and that ACL was likely obligated to notify the Commissioner and affected individuals.

37 In the period between 22 June 2022 and 10 July 2022, Clyde & Co, at the direction of ACL, accessed and conducted an initial review of the Medlab data which had been exfiltrated and published.

38 On 10 July 2022, ACL provided a statement under s 26WK of the Act to the Commissioner, informing her that ACL had reasonable grounds to believe that the Medlab Cyberattack amounted to an "eligible data breach" in respect of the Medlab IT Systems (within the meaning of s 26WE of the Act). The statement confirmed:

> …Once the cyber security investigation is completed, Medlab will take appropriate steps to update the OAIC and notify any potentially affected individuals in accordance with 26WL(2) of the [Act]…

39 On 27 October 2022, ACL made an ASX announcement and published it on its website relating to the Medlab Cyberattack, in which it offered a public apology from its CEO, provided details of the notification process and support services for affected individuals and confirmed that ACL would continue to work with the relevant authorities in relation to the Medlab Cyberattack.

C. CONTRAVENTIONS OF S 13G BY REASON OF BREACH OF APP 11.1(B)

Statutory provisions and relevant principles

Section 13G of the Act

40 Section 13G provides:

> **13G Serious and repeated interferences with privacy**
>
> An entity contravenes this subsection if:
>
> (a) the entity does an act, or engages in a practice, that is a serious interference with the privacy of an individual; or
>
> (b) the entity repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals.
>
> Civil penalty: 2,000 penalty units.

Contravention of s 13G(a) by reason of a breach of APP 11.1(b)

41 Section 13 of the Act relevantly provides:

> **13 Interferences with privacy**
>
> APP entities
>
> (1) An act or practice of an APP entity is an interference with the privacy of an individual if:
>
> (a) the act or practice breaches an Australian Privacy Principle in relation to personal information about the individual…

42 Section 14 of the Act provides that the APPs are set out in the clauses of Sch 1.

43 Section 15 of the Act provides that an APP entity (as it is defined in s 6(1) of the Act) must not do an act, or engage in a practice, that breaches an APP. Section 6A also provides that, for the purposes of the Act, an act or practice breaches an APP if, and only if, it is contrary to, or inconsistent with, that principle.

44 The following terms are defined in s 6(1) of the Act:

(a) "APP entity" is defined as meaning an agency or organisation.

(b) "Personal information" is defined as meaning information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(i) whether the information is true or note; and

(ii) whether the information is recorded in a material form or not.

(c) "Individual" is defined as meaning a natural person.

(d) "Holds" is defined as:

> an entity holds personal information if the entity has possession or control of a record that contains the personal information.

(e) "Record" is defined as including, relevantly, a document or an electronic or other device.

45 Section 6C(1) of the Act defines an "organisation" as including a body corporate.

46 It follows from the above that, to the extent an APP entity engages in an act or practice that breaches an APP in relation to personal information about an individual, that act or practice is an interference with the privacy of that individual under s 13(1)(a) of the Act. If that interference is serious, then the APP entity also contravenes s 13G(a).

APP 11.1(b)

47 The relevant APP in the present proceeding is APP 11.1(b), which is set out in Sch 1 of the Act.

48 APP 11.1(b) has not been the subject of any previous judicial consideration.

49 APP 11.1(b) requires an APP entity that holds "personal information" to take "such steps as are reasonable in the circumstances" to protect personal information from "unauthorised access, modification or disclosure". It raises for consideration the scope of the "circumstances" to be taken into account and the question as to what actions may be sufficient to constitute "reasonable steps" under the Act.

50 Textually, APP 11.1(b) provides that an objective standard is to be applied to determine the steps that are required to be undertaken and necessarily the scope of those steps must be informed by the circumstances. There is no reason textually why the circumstances should not be given a broad construction. The circumstances could be expected to include the sensitivity

of the personal information, the potential harm to individuals if the information was accessed or disclosed, the size and sophistication of the APP entity, the cybersecurity environment in which the APP entity operates, and any previous threats or cyberattacks made against the APP entity.

51 The breadth of the necessary inquiry into what might constitute "such steps as are reasonable in the circumstances" is informed by judicial consideration of other legislation that import a "reasonable steps" obligation, in particular, s 961L, s 963F and s 994E(5) of the *Corporations Act 2001* (Cth) (**Corporations Act**). The obligation has been stated:

(a) to differ depending on the complexity of the entity's business and the procedures within the entity: *Australian Securities and Investments Commission v Healey* (2011) 196 FCR 291; [2011] FCA 717 at [162] (Middleton J);

(b) not to be capable of being discharged simply by delegating it to another entity and doing nothing more: *Clarke (as trustee of the Clarke Family Trust) & Ors v Great Southern Finance Pty Ltd (Receivers and Managers Appointed) (in liquidation) & Ors* [2014] VSC 516 at [543] (Croft J);

(c) to require a wholistic analysis, considering the full framework of the entity's systems, policies and procedures: *Australian Securities and Investments Commission v Diversa Trustees Limited* [2023] FCA 1267 at [375] (Button J);

(d) not to require a person to find and take the optimal steps: *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (No 2)* [2021] FCA 877; (2021) 156 ACSR 371 at [392] (Moshinsky J);

(e) not to require a person to take *all* reasonable steps, nor to identity the universe of possible reasonable steps or the "one true path" to be followed; the focus of the inquiry must always be on whether the steps that were taken in their totality were reasonable: *Australian Securities and Investments Commission v R M Capital Pty Ltd* [2024] FCA 151; (2021) 172 ACSR 1 at [73] and [80] (Jackson J);

(f) to be assessed objectively by reference to the standard of behaviour expected of a reasonable person in the regulated person's position: *Australian Securities and Investments Commission v Firstmac Limited* [2024] FCA 737 at [51] (Downes J).

Consideration

52 I am satisfied that the agreed facts and admissions the subject of the SAFA and summarised at [10] to [39] above establish that ACL did not take "such steps as are reasonable in the circumstances" to protect the personal information held on the Medlab IT Systems from, relevantly, "unauthorised access" and "unauthorised disclosure", in particular having regard to (a) the size and nature of the business of ACL; (b) the volume and sensitivity of the information; (c) the high cybersecurity risks facing ACL during the Relevant Period and the risk of harm to individuals if their health and other personal information held by ACL on the Medlab IT Systems was accessed and disclosed without authorisation, (d) the Medlab IT Systems Deficiencies, (e) ACL's failure to identify the Medlab IT Systems Deficiencies prior to their acquisition, (f) the delay in ACL identifying the Medlab IT Systems Deficiencies, and (g) the overreliance that ACL placed on third party service providers and its failure to have in place adequate procedures to detect and respond by itself to cyber incidents.

53 As ACL has admitted in the SAFA, its ability to detect and respond by itself to cyber incidents was deficient because (a) 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, (b) there was inadequate testing of incident management processes in the period between the acquisition of the Medlab IT Systems and the Medlab Cyberattack, (c) 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, (d) 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, (e) there was no application whitelisting in place to prevent unknown or unauthorised applications from running on Medlab computers, (f) there were only limited communications plans, (g) 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, (h) there was limited security monitoring capability because the firewall logs were only retained for one hour, (i) specific data recovery plans had not been developed, and (j) Medlab staff were not required to use multifactor identification to use the Medlab VPN (together, **Medlab Cyberattack Response Deficiencies**).

54 For these reasons, I am satisfied that ACL breached APP 11.1(b) of the Act, and, by reason of s 13(1)(a) of the Act, that breach constituted an interference with the privacy of more than 223,000 individuals whose personal information ACL held on the Medlab IT Systems.

55 Further, I am satisfied that the breaches of privacy of those 223,000 individuals were serious for the purposes of s 13G(a) of the Act.

56 There is no definition of "serious" or "serious contravention" in the Act. Nor is "serious contravention" defined in either the *Australian Securities and Investments Act 2001* (Cth) (**ASIC Act**) or the Corporations Act.

57 For the purposes of the ASIC Act and the Corporations Act, a "serious contravention" has been construed as a contravention that is "grave or significant" or "weighty, important, grave and considerable", and, in every case, it is ultimately a question of fact to be determined by reference to the degree of the departure from the requisite standard of care and diligence and the nature of the conduct, rather than the nature of the provision that has been contravened: *Provide Nominees Pty Ltd v Australian Securities and Investments Commission* [2024] FCA 303 at [47]-[53] (Rofe J), in which her Honour agreed with the reasoning of both Ipp JA in *Vines v Australian Securities and Investments Commission* [2007] NSWCA 126; (2007) 63 ACSR 505 at [229] and Lee J in *Australian Securities and Investments Commission v GetSwift Ltd (Penalty Hearing)* (2023) [2023] FCA 100; 167 ACSR 178 at [54].

58 I am satisfied that, applying those principles, as jointly submitted by the parties, the "serious" threshold has been met, particularly having regard to the nature and volume of the personal information, including sensitive health information held on the Medlab IT Systems, the extent of the Medlab IT System Deficiencies, and the Medlab Cyberattack Response Deficiencies, and ACL's reliance on a third party cybersecurity services provider, all of which significantly heightened the risk that the personal information would be exposed to unauthorised access.

59 It is next necessary to determine the number of contraventions arising from the breach of APP 11.1(b).

60 The parties have agreed, and I am satisfied, that ACL engaged in a separate contravention of s 13G(a) in respect of each of the more than 223,000 individuals, whose personal information was held on the Medlab IT Systems during the Relevant Period.

61 The objects of the Act, as stated in s 2A, make plain that the Act is directed primarily at the "protection of the privacy of individuals" – not the acts or practices that might breach APPs.

That emphasis is also consistent with the following statement in the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) on the proposed s 13G to the Act:

> Section 13G will implement the Government's response to ALRC Recommendation 50-2, by creating a civil penalty where an entity does an act or engages in a practice which is a serious interference with *the privacy of an individual*, or where the entity repeatedly does an act, or engages in a practice that is an interference with *the privacy of one or more individuals*.
>
> (emphasis added)

62 Textually, s 13(1)(a) is directed at "an interference with the privacy of *an* individual" if the act or practice of the APP entity breaches an APP "in relation to personal information about *the* individual" (emphasis added). In turn, s 13G(a) is directed at "a *serious* interference with the privacy of *an* individual" (emphasis added). In contrast, s 13G(b) is directed at "an interference with the privacy of *one or more* individuals" (emphasis added). Section 13G provides for the imposition of a civil penalty for a serious interference with the privacy of *an* individual (s 13G(a)) or if an entity repeatedly does an act or engages in a practice, that is an interference with the privacy of *one or more* individuals (s 13G(b)).

D. CONTRAVENTION OF S 13G BY REASON OF CONTRAVENTION OF S 26WH(2)

Statutory provisions and relevant principles

63 For there to be a contravention of s 26WH(2) of the Act, there must have been an "eligible data breach".

64 The concept of an "eligible data breach" is addressed in Div 2 of Pt IIIC of the Act. It is defined in s 26WE(2) and relevantly applies if under s 26WE(1)(a):

> (a) both:
>
> (i) an APP entity holds personal information relating to one or more individuals; and
>
> (ii) the APP entity is required under section 15 not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information;

65 Section 26WE(2) provides:

> (2) For the purposes of this Act, if:
>
> (a) both of the following conditions are satisfied:
>
> (i) there is unauthorised access to, or unauthorised disclosure of,

the information;

(ii) a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or

(b) the information is lost in circumstances where:

(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and

(ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates;

then:

(c) the access or disclosure covered by paragraph (a), or the loss covered by paragraph (b), is an ***eligible data breach*** of the APP entity...; and

(d) an individual covered by subparagraph (a)(ii) or (b)(ii) is ***at risk*** from the eligible data breach.

66 Section 26WF(1) provides that if the APP entity takes action in relation to the access or disclosure of information covered by s 26WE(2)(a) before any individual to whom the information relates has suffered any serious harm, and that as a result of that action, a reasonable person would conclude that the access or disclosure was not likely to result in serious harm to any of those individuals, then the access or disclosure is deemed not to be an "eligible data breach".

67 Section 26WG provides that for the purposes of Div 2 of Pt IIIC of the Act, in determining whether a reasonable person would conclude that an access to, or disclosure of, information would be likely or not likely to result in serious harm to any individuals to whom the information relates, the Court must have regard to the matters identified in the following subparagraphs of s 26WG:

(c) the kind or kinds of information;

(d) the sensitivity of the information;

(e) whether the information is protected by one or more security measures;

(f) if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;

(g) the persons, or the kinds of persons, who have obtained, or who could obtain, the information;

(h) if a security technology or methodology:

(i) was used in relation to the information; and

(ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;

the likelihood that the persons, or the kinds of persons, who:

(iii) have obtained, or who could obtain, the information; and

(iv) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;

(i) the nature of the harm;

(j) any other relevant matters.

68 Division 3 of Part IIIC provides a scheme for the notification of eligible data breaches.

69 Section 26WH provides:

Scope

(1) This section applies if:

(a) an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity; and

(b) the entity is not aware that there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity.

Assessment

(2) The entity must:

(a) carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and

(b) take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware as mentioned in paragraph (1)(a).

…

70 Section 26WH is engaged if an APP entity is aware that there were reasonable grounds *to suspect* that there may have been an eligible data breach but is not aware that there are reasonable grounds to believe that there was an eligible data breach.

71 If s 26WH is engaged, then the APP entity is required to carry out a reasonable and expeditious assessment of whether there are reasonable grounds *to believe* that the unauthorised access

amounted to an eligible data breach and take all reasonable steps to ensure that the assessment is completed within 30 days.

72 Section 13(4A) of the Act relevantly provides that if an APP entity contravenes s 26WH(2), that is taken to be an act that is "an interference with the privacy of an individual".

73 If the contravention is serious, the APP entity contravenes s 13G(a) of the Act, because it is relevantly engaged if an entity does an act that is a "serious interference with the privacy of an individual".

Consideration

74 I am persuaded that the facts agreed and the admissions made in the SAFA are sufficient to establish that by 2 March 2022, ACL had subjective knowledge or awareness of circumstances, notwithstanding StickmanCyber's advice to the contrary, that were objectively sufficient to establish in the mind of a reasonable person a suspicion that (a) there may have been unauthorised access to the personal and sensitive information of individual customers and patients held on the Medlab IT Systems over which ACL had control at that time, and (b) that access would be likely to result in serious harm to any of the over 223,000 individuals to whom the information related.

75 I am satisfied that this knowledge or awareness of ACL was sufficient to give rise to the requisite state of suspicion under s 26WH(1), by reason of s 26WH(2) of the Act, and thereby requires ACL to carry out a reasonable and expeditious assessment to determine whether there were reasonable grounds to believe that the Medlab Cyberattack amounted to an eligible data breach, and to take all reasonable steps to complete that assessment within 30 days of 2 March 2022.

76 I am also persuaded the facts agreed and the admissions made in the SAFA are sufficient to establish that ACL did not carry out such an assessment and thereby contravened s 26WH(2) of the Act for the following reasons.

77 *First*, the assessment undertaken by StickmanCyber that was relied upon by ACL was inadequate because it (a) only monitored 3 of the at least 127 computers subject to ransomware deployed by the Quantum Group, (b) did not conduct any investigation into the Quantum Group and its attack traits to determine whether data was likely to have been exfiltrated, (c) based its review on only one of the firewall logs, which it did not access until approximately four hours after the ransom demand was first downloaded, and (d) only conducted a limited investigation

of whether the Quantum Group may have established a persistence mechanism to stay connected to the Medlab IT Systems and its network.

78 *Second*, ACL was aware of the limited assessment undertaken by StickmanCyber and it was therefore unreasonable for ACL to rely solely on that assessment and StickmanCyber's advice to conclude by 2 March 2022 that the threat posed by the Medlab Cyberattack had been contained and that there was no information which suggested that personal information held by the Medlab IT Systems had been exfiltrated.

79 Further, I am persuaded that the contravention by ACL of s 26WH(2) was serious, in particular because of (a) the sensitivity and volume of the personal information held on the Medlab IT Systems, (b) the high cybersecurity risks facing ACL during the Relevant Period, and (c) the fact that the failure to conduct the stipulated reasonable and expeditious assessment likely resulted in a delay in ACL ultimately notifying the Commissioner on 10 July 2022 that there were reasonable grounds to believe that there had been an eligible data breach and thereby delayed the ability to the Commissioner to perform her statutory function of monitoring ACL's notification to individuals whose personal information may have been compromised.

80 I am therefore satisfied that ACL engaged in a single contravention of s 13G(a) of the Act by reason of its contravention of s 26WH(2) of the Act.

E. CONTRAVENTION OF S 13G BY REASON OF CONTRAVENTION OF S 26WK(2)

Statutory provisions and relevant principles

81 Section 26WK is engaged if an APP entity is aware that there are reasonable grounds *to believe* that there has been an eligible data breach.

82 Section 26WK provides:

> *Scope*
>
> (1) This section applies if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.
>
> *Statement*
>
> (2) The entity must:
>
> (a) both:
>
> (i) prepare a statement that complies with subsection (3); and
>
> (ii) give a copy of the statement to the Commissioner; and

(b) do so as soon as practicable after the entity becomes so aware.

(3) The statement referred to in subparagraph (2)(a)(i) must set out:

(a) the identity and contact details of the entity; and

(b) a description of the eligible data breach that the entity has reasonable grounds to believe has happened; and

(c) the kind or kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

(4) If the entity has reasonable grounds to believe that the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more other entities, the statement referred to in subparagraph (2)(a)(i) may also set out the identity and contact details of those other entities.

83 If s 26WK is engaged, then the APP entity must prepare and provide a statement to the Commissioner that sets out the information stipulated in subsection (3) as soon as practicable after the entity becomes so aware.

84 Section 13(4A) of the Act relevantly provides that if an APP entity contravenes s 26WK(2), that is taken to be an act that is "an interference with the privacy of an individual".

85 If the contravention is serious, the APP entity contravenes s 13G(a) of the Act, because it is relevantly engaged if an entity does an act that is a "serious interference with the privacy of an individual".

Consideration

86 I am persuaded by the facts agreed and the admissions made in the SAFA that by at least the date of the second ACSC notification on 16 June 2022, ACL had reasonable grounds to believe that there had been an eligible data breach, and its obligation to report the Medlab Cyberattack to the Commissioner as soon as practicable was thereby engaged.

87 There is no definition of "practicable" in the Act. The Explanatory Memorandum to the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (Cth) which introduced Part IIIC into the Act, however, provides the following guidance:

> …'Practicability' in the context of paragraphs 26WL(2)(a)−(c) is intended to involve considerations about whether the time, effort or cost of a particular form of notification, when considered in all the circumstances of the entity and the data breach, would render such notification impracticable…

88 In assessing the time, effort, or cost of a particular notification under s 26WL(2) of the Act, it is readily apparent that the information required to be included in a notification is not particularly onerous and is intended to facilitate the provision of the notification as "soon as practicable" after the entity becomes aware of reasonable grounds to believe that there has been an eligible data breach. The notification only needs to provide a description of the data breach, the kind or kinds of information concerned, and recommendations about the steps that individuals should take in response to the eligible data breach.

89 ACL admits in the SAFA, and I am satisfied, that it was practicable for it to have prepared a statement that complied with s 26WK(3) of the Act and to have provided a copy to the Commissioner within two to three days of it becoming aware on 16 June 2022 of reasonable grounds to believe that there had been an eligible data breach.

90 A statement pursuant to s 26WK(3) was not provided by ACL to the Commissioner until 10 July 2022. I am therefore satisfied that ACL contravened s 26WK(2) of the Act.

91 I am also persuaded that the contravention of s 26WK(2) was serious, in particular, because of (a) the sensitivity and volume of the personal information held on the Medlab IT Systems, (b) the high cybersecurity risks facing ACL during the Relevant Period, (c) the fact that the delay in ACL providing the s 26WK(3) notification to the Commissioner on 10 July 2022 delayed the ability of the Commissioner to perform her statutory function of monitoring ACL's notification to individuals whose personal information may have been compromised, providing guidance and information about the impact of the Medlab Cyberattack and engaging with other Government agencies.

92 I am therefore satisfied that ACL engaged in a single contravention of s 13G(a) of the Act by reason of its contravention of s 26WK(2) of the Act.

F. DECLARATIONS OF CONTRAVENTION BY ACL

Relevant principles

93 The Court has a wide discretionary power to make declarations under s 21 of the *Federal Court of Australia Act 1976* (Cth): *Forster v **Jododex** Australia Pty Ltd* (1972) 127 CLR 421 at 437-8 (Gibbs J); *Ainsworth v Criminal Justice Commission* (1992) 175 CLR 564 at 581-2 (Mason CJ, Dawson, Toohey and Gaudron JJ).

94 Before making a declaration, including a declaration by consent, the Court must be satisfied that (a) the question must be a real and not a hypothetical or theoretical one, (b) the applicant must have a real interest in raising it, and (c) there must be a proper contradictor: *Jododex* at 437-8 (Gibbs J).

95 A respondent who has a real interest in opposing a declaration may be a proper contradictor notwithstanding that it consents to the making of the declaration: *Australian Competition and Consumer Commission v MSY Technology Pty Ltd* (2012) 201 FCR 378; [2012] FCAFC 56 at [30].

96 The Court should pay close attention to the form of declarations, particularly declarations made "by consent", and should ensure that the declarations outline the "gist" of the Court's findings identifying the contravening conduct: *Rural Press Ltd v Australian Competition and Consumer Commission* (2003) 216 CLR 53; [2003] HCA 75 at [89]-[90] (Gummow, Hayne and Heydon JJ).

97 It is well established that declarations of contraventions of legislative provisions are likely to be appropriate where they (a) record the Court's disapproval of the contravening conduct, (b) vindicate a regulator's claim that a respondent contravened the provisions, (c) assist a regulator in performing its duties, and (d) deter other persons from contravening the provisions: *Australian Securities and Investments Commission v Macquarie Bank Limited* [2024] FCA 416 at [57] (Wigney J).

98 The Court must be independently satisfied that a contravention has occurred before making a declaration that a civil penalty provision has been contravened, but the material which may produce that satisfaction may include a statement of agreed facts and admissions: *Australian Securities and Investments Commission v Rich* [2004] NSWSC 836; (2004) 50 ACSR 500 at [15] (White J).

Consideration

99 I am satisfied that the facts agreed and admissions made in the SAFA are sufficient to establish that ACL has contravened s 13G(a) by reason of its breaches of APP 11.1(b), and s 26 WH(2) and s 26WK(2) of the Act, and that the proposed declarations of contravention should be made for the following reasons.

100 *First*, the questions raised in the proposed declaration are real questions of practical importance given that they (a) resolve the controversy concerning ACL's conduct during the Relevant

Period in response to the Medlab Cyberattack, and (b) will assist APP entities in understanding the scope and extent of their obligations to protect sensitive private information from unauthorised access.

101 *Second*, the Commissioner, as a regulator, has a real interest in raising the questions, and there is a public interest in judicial guidance being provided to APP entities as to the scope and nature of their responsibilities under the Act to protect, and have in place appropriate systems and procedures to protect personal information of individuals.

102 *Third*, ACL is a proper contradictor and has a real interest in opposing relief, notwithstanding that it has now agreed the facts and made the admissions in the SAFA.

103 *Fourth*, the proposed declarations will provide a public indication of the seriousness with which the Court views the contraventions by ACL of its obligations to protect personal information of individuals from unauthorised access, vindicate the Commissioner's claims that the conduct of ACL was unsatisfactory, and deter other APP entities from contravening the Act.

104 *Fifth*, the agreed terms of the proposed declarations adequately identify the conduct that constituted the contraventions.

G. THE PECUNIARY PENALTY TO BE PAID BY ACL

Statutory provisions and relevant principles

Pecuniary penalties

105 Section 80U of the Act provides that each civil penalty of the Act is enforceable by the Commissioner as an "authorised applicant" under Pt 4 of the *Regulatory Powers (Standard Provisions) Act 2014 (Cth)* (**Regulatory Powers Act**).

106 The relevant provisions of Pt 4 of the Regulatory Powers Act provide:

> **82 Civil penalty orders**
>
> Application for order
>
> (1) An authorised applicant may apply to a relevant court for an order that a person, who is alleged to have contravened a civil penalty provision, pay the Commonwealth a pecuniary penalty.
>
> […]
>
> *Court may order person to pay pecuniary penalty*
>
> (3) If the relevant court is satisfied that the person has contravened the civil penalty provision, the court may order the person to pay to the

Commonwealth such pecuniary penalty for the contravention as the court determines to be appropriate.

[…]

Determining pecuniary penalty

(5) The pecuniary penalty must not be more than:

(a) if the person is a body corporate—5 times the pecuniary penalty specified for the civil penalty provision; and

(b) otherwise—the pecuniary penalty specified for the civil penalty provision.

(6) In determining the pecuniary penalty, the court must take into account all relevant matters, including:

(a) the nature and extent of the contravention; and

(b) the nature and extent of any loss or damage suffered because of the contravention; and

(c) the circumstances in which the contravention took place; and

(d) whether the person has previously been found by a court (including a court in a foreign country) to have engaged in any similar conduct.

[…]

85 Multiple contraventions

(1) A relevant court may make a single civil penalty order against a person for multiple contraventions of a civil penalty provision if proceedings for the contraventions are founded on the same facts, or if the contraventions form, or are part of, a series of contraventions of the same or a similar character.

…

(2) However, the penalty must not exceed the sum of the maximum penalties that could be ordered if a separate penalty were ordered for each of the contraventions.

107 In addition to the mandatory factors in s 82(6) of the Regulatory Powers Act, the so-called "*French* factors" enunciated by French J in *Trade Practices Commission v CSR Limited* [1990] FCA 521 at [42], expanded upon by his Honour in *Australian Securities and Investments Commission v Chemeq Ltd* [2006] FCA 936 at [99] and then elaborated on in further decisions, including, for instance, *Australian Securities and Investments Commission v Westpac Banking Corporation (No 3)* [2018] FCA 1701 at [49] (Beach J), should be considered.

108 These factors, as applicable to the present case and contraventions, include:

(a) the extent to which the contravention was the result of deliberate or reckless conduct by the corporation, as opposed to negligence or carelessness;

(b) the number of contraventions, the length of the period over which the contraventions occurred, and whether the contraventions comprised isolated conduct or were systematic;

(c) the seniority of those responsible for the contravention and whether the directors and senior management of the contravener were aware of the relevant facts and, if not, what processes were in place at the time or put in place after the contravention to ensure their awareness of such facts in the future;

(d) the size and financial position of the contravener for the purpose of informing the size of the pecuniary penalty that would operate as an effective specific deterrent;

(e) the existence within the corporation of compliance systems, including provisions for and evidence of education and internal enforcement of such systems and whether the entity had a culture of compliance;

(f) remedial steps taken after the contravention and directed to putting in place a compliance system or improving existing systems and disciplining officers responsible for the contravention;

(g) the degree of the entity's cooperation with the regulator, including any admission of an actual or attempted contravention;

(h) the impact or consequences of the contravention on the market or innocent third parties; and

(i) the extent of any profit or benefit derived as a result of the contravention.

109 If the Court is satisfied that there has been a contravention of a civil penalty provision, it then has a discretion to order the contravener to pay a pecuniary penalty.

110 The following general principles governing the exercise of that discretion can be distilled from the authorities as relevantly applicable to the imposition of a pecuniary penalty for a contravention of s 13G(a) of the Act.

111 *First,* "the purpose of a civil penalty is primarily, if not solely, the promotion of the public interest in compliance with the provisions of the [Act] by the deterrence of further contraventions of the [Act]": *Australian Building and Construction Commissioner v* ***Pattinson*** (2022) 274 CLR 450; [2022] HCA 13 at [9].

112 *Second*, the power to order a penalty under s 82(3) of the Regulatory Powers Act is a discretionary one which must be exercised judicially, having regard to the subject matter, scope, and purpose of the legislation: *Pattinson* at [40].

113 *Third*, the process of fixing the quantum of a penalty is one of "instinctive synthesis", addressing many conflicting and contrasting considerations: *Australian Competition and Consumer Commission v Reckitt Benckiser (Australia) Pty Ltd* [2016] FCAFC 181 at [44] (Jagot, Yates and Bromwich JJ).

114 *Fourth*, a civil penalty must be fixed with a view to ensuring that the penalty is not such as to be regarded by the contravener (or others) as an acceptable cost of doing business: *Australian Competition and Consumer Commission v TPG Internet Pty Ltd* (2013) 250 CLR 640; [2013] HCA 54 at [66] (French CJ, Crennan, Bell and Keane JJ), quoting *Singtel Optus Pty Ltd v Australian Competition and Consumer Commission* [2012] FCAFC 20 at [62] (Keane CJ, Finn and Gilmour JJ).

115 *Fifth*, the penalty to be imposed must be proportionate in a sense that it must strike a reasonable balance between deterrence and oppressive severity: *Pattinson* at [41].

116 *Sixth*, the "course of conduct" or "one transaction" principle requiring consideration of whether the subject contraventions arise out of the same course of conduct or the same transaction may inform the Court's determination of an appropriate penalty: *Australian Competition and Consumer Commission v Yazaki Corporation* (2018) 262 FCR 243, [2018] FCAFC 73 at [234] (Allsop CJ, Middleton and Robertson JJ) .

Agreed penalties

117 It has long been recognised that there is an important public policy involved in promoting the predictability of outcomes in civil penalty proceedings. The practice of receiving and, if appropriate, accepting agreed penalty submissions increases the predictability of outcomes for regulators and wrongdoers encourages corporations to admit contraventions, assists in avoiding lengthy and complex litigation, and enables regulators to pursue other areas of investigation: *Commonwealth v Director, Fair Work Building Industry Inspectorate* (2015) 258 CLR 482; [2015] HCA 46 at [46] (French CJ, Kiefel, Bell, Nettle and Gordon JJ).

118 The following principles governing the approach by the Court to the consideration of agreed proposed penalties can be distilled from the decision of the Full Court in *Volkswagen*

Aktiengesellschaft v Australian Competition and Consumer Commission (2021) 284 FCR 24; [2021] FCAFC 49 at [124]-[131] (Wigney, Beach and O'Bryan JJ):

(a) there is no single appropriate penalty, rather, there is a permissible range of penalties, determined by all the relevant facts and circumstances, within which no particular figure can necessarily be said to be more appropriate than another (at [127]);

(b) the Court should generally recognise that an agreed proposed penalty is most likely the result of compromise and pragmatism on the part of the regulator and reflects the regulator's considered estimation of the penalty necessary to achieve deterrence and the risks and expenses of the litigation had it not been settled (at [129]; and

(c) if the proposed penalty falls within the permissible or acceptable range, the public policy consideration of predictability of outcome will generally provide a compelling reason for the Court to accept the proposed penalty (at [131]).

119 Further, it has been observed that judicial restraint is likely to be particularly appropriate where the parties are sophisticated, legally represented, and well able to understand and evaluate the desirability of the settlement: *Australian Competition and Consumer Commission v Colgate-Palmolive Pty Ltd (No 3)* [2016] FCA 676 at [27] (Jagot J).

Consideration

120 As explained above, during the Relevant Period s 13G(a) of the Act attracted a maximum civil penalty of 2,000 penalty units, and s 82(5)(a) of the Regulatory Powers Act provided that the pecuniary penalty for a body corporate must not be more than five times the pecuniary penalty specified for the civil penalty provision. Further, during the Relevant Period, the value of a penalty unit was set at $222.00: s 4AA of the *Crimes Act 1914* (Cth).

121 The parties have agreed a penalty of (a) $4.2 million for the 223,000 contraventions of s 13G(a) by reason of the breaches of APP 11.1 against a maximum penalty of $495,060,000,000, (b) $800,000 for the single contravention of s 13G(a) by reason of the contravention of s 26WH(2) against a maximum penalty of $2.2 million, and (c) $800,000 for the single contravention of s 13G(a) by reason of the contravention of s 26WH(2) against a maximum penalty of $2.2 million.

122 I am persuaded that in aggregate, the agreed penalty of $5,800,000 is appropriate in all the circumstances. I am satisfied for the following principal reasons that it falls within the range of

permissible penalties that the Court could impose in this case for the contraventions by ACL of s 13G(a) in the context of the agreed facts and admissions in the SAFA.

123 *First*, the contraventions were extensive and significant. The cybersecurity controls of the Medlab IT Systems were under the control of ACL from the commencement of the Relevant Period and were deficient from at least the time the assets of Medlab were acquired. The Medlab IT Systems Deficiencies, to the knowledge of ACL, exposed the Medlab IT Systems to the risk of a cyberattack during the six-month period in which ACL was integrating them into ACL's core IT network. That risk materialised in the Medlab Cyberattack in which personal and sensitive information of at least 223,000 individuals, including passport numbers, health information and financial information, was compromised and, on or before 16 June 2022, posted on the dark web.

124 *Second*, ACL's contraventions of s 13G(a) of the Act resulted from its failure to act with sufficient care and diligence in managing the risk of a cyberattack on the Medlab IT Systems.

125 *Third*, although it is not possible to quantify the loss or damage caused by ACL's contravening conduct, I am satisfied that the contraventions, given the nature of the information posted on the dark web, had at least the potential to cause significant harm to individuals whose information had been exfiltrated, including financial harm, distress or psychological harms, and material inconvenience.

126 *Fourth*, and relatedly, the contraventions had the potential to have a broader impact on public trust in entities holding private and sensitive information of individuals, including the capability of those entities to identify and report eligible data breaches to the Commissioner in a timely fashion to enable her to perform her statutory functions, including monitoring of steps to be taken to notify affected individuals to enable them to take actions to protect themselves from the harm, loss, and damage associated with the eligible data breaches.

127 *Fifth*, relevantly for personal deterrence, ACL is and was during the Relevant Period, one of Australia's largest private hospital pathology businesses, generating (a) revenue of $674.4 million and net profit of $88.7 million in the financial year ending 30 June 2021, (b) revenue of $995.6 million and net profit of $178.2 million in the financial year ending 30 June 2022, and (c) revenue of $697.1 million and net profit of $41.7 million in the financial year ending 30 June 2023.

128 *Sixth*, ACL's most senior management were involved in the decision making around the integration of Medlab's IT Systems into ACL's core environment and ACL's response to the Medlab Cyberattack, including whether it amounted to an eligible data breach.

129 The matters summarised above would suggest that a penalty of $5.8 million was manifestly inadequate or at least outside an acceptable or permissible range to achieve specific and general deterrence. The significance of these matters, however, needs to be weighed against the following ameliorating considerations.

130 *First*, ACL did not derive financial gain or benefit from the contraventions.

131 *Second*, ACL has not previously been found by a Court to have contravened the Act or otherwise engaged in any similar conduct.

132 *Third*, there is no suggestion that any of the contraventions were deliberate or arose from any deliberate misconduct of any of ACL's senior management.

133 *Fourth*, ACL had commenced a review of its cybersecurity processes and controls prior to the Medlab Cyberattack, and the ACL board had approved in July 2021 a program of works to uplift the company's cybersecurity capabilities. The program included a requirement since August 2022 that all ACL employees undertake regular cybersecurity awareness training through a specialist third party vendor. Further, in August 2023, ACL appointed an experienced and credentialled full-time Chief Information Security Officer. I am satisfied that these actions demonstrate that ACL has sought, and continues to seek, to take meaningful steps to develop a satisfactory culture of compliance.

134 *Fifth*, ACL has cooperated with the investigation undertaken by the office of the Commissioner since around December 2022 into the acts and practices of ACL and Medlab in relation to the Medlab Cyberattack, including producing multiple written responses and some 12,000 documents.

135 *Sixth*, following the commencement of this proceeding and prior to the scheduled hearing on liability, ACL has admitted the contraventions the subject of the proceeding by way of the filing of the SAFA.

136 *Seventh*, the CEO of ACL apologised that the Medlab Cyberattack had occurred in the terms set out in the 27 October 2022 ASX announcement.

137 *Eighth,* although I have concluded that there were approximately 223,000 contraventions of s 13G(a) arising from the breach by ACL of APP 11.1(b), I am satisfied that the contraventions arose from a single course of conduct, being the failure to have in place adequate cybersecurity controls to protect individuals' personal information held on the Medlab IT Systems.

138 I am persuaded that, having regard to all these matters, the totality principle which operates as a final check and the need to avoid a penalty that is oppressively severe, an aggregate penalty of $5.8 million falls within the range of permissible penalties to achieve both specific and general deterrence. Further, as for specific deterrence, I am satisfied that the penalties could not objectively be characterised as "a cost of doing business" and, as for general deterrence, the penalty is sufficient to send an appropriate deterrent signal to participants in the healthcare system as to their responsibilities in protecting sensitive personal information in the course of conducting their businesses, particularly given this is the first civil penalty proceeding brought by the Commissioner in the history of the Act.

H. DISPOSITION

139 Declarations in the form sought by the Commissioner and agreed by ACL with respect to ACL's contraventions of s 13G(a) of the Act will be made.

140 ACL will also be ordered to pay a civil penalty in aggregate of $5,800,000 in respect of its contraventions of s 13G(a) of the Act.

141 The parties have also agreed that ACL is to pay a contribution of $400,000 towards the Commissioner's costs of the proceeding.

I certify that the preceding one hundred and forty-one (141) numbered paragraphs are a true copy of the Reasons for Judgment of the Honourable Justice Halley.

Associate:

Dated: 8 October 2025

Annexure A

Federal Court of Australia
District Registry: New South Wales
Division: General

No: NSD1287/2023

AUSTRALIAN INFORMATION COMMISSIONER
Applicant

AUSTRALIAN CLINICAL LABS LIMITED (ACN 645 711 128)
Respondent

STATEMENT OF AGREED FACTS AND ADMISSIONS

A. INTRODUCTION

1. The Applicant, the Australian Information Commissioner (**Commissioner**) and the Respondent, Australian Clinical Labs Limited (**ACL**) agree, pursuant to s 191 of the *Evidence Act 1995* (Cth), that the facts stated in this Statement of Agreed Facts and Admissions (**SAFA**) are not, for the purposes of this proceeding, disputed.

2. This SAFA supersedes the Statement of Agreed Facts made in this proceeding on 14 June 2024.

B. THE PARTIES

The Commissioner

3. The Commissioner:

   a. is the Australian Information Commissioner appointed under s 14 of the *Australian Information Commissioner Act 2010* (Cth) (the **Australian Information Commissioner Act**); and

   b. is the Head of the Office of the Australian Information Commissioner, a statutory agency established under s 5 of the Australian Information Commissioner Act.

Filed on behalf of (name & role of party) Australian Information Commissioner
Prepared by (name of person/lawyer) John Fogarty
Law firm (if applicable) DLA Piper Australia
Tel 03 9274 5080 Fax
Email john.fogarty@dlapiper.com
Address for service (include state and postcode) Level 14, 80 Collins Street, Melbourne, VIC 3000

[Form approved 01/08/2011]

4. The Commissioner's functions are prescribed by Division 3 of Part 2 of the Australian Information Commissioner Act and include the "privacy functions" within the meaning of s 9 thereof.

ACL

5. ACL was incorporated on 6 November 2020 and is a public company listed on the Australian Securities Exchange (**ASX**).

6. ACL replaced Clinical Laboratories Pty Ltd (**Clinical Labs**) as the ultimate holding company of the ACL group of companies on 17 December 2020.

7. ACL is, and was during the period from 19 December 2021 to 15 July 2022 (**Relevant Period**), one of the largest private hospital pathology businesses in Australia, generating revenue of:

   a. $674.4 million in the financial year ending June 2021;

   b. $995.6 million in the financial year ending June 2022; and

   c. $697.1 million in the financial year ending June 2023.

8. As at 30 June 2022, ACL employed approximately 5,400 staff. As at 30 June 2023, ACL employed approximately 5,115 staff.

9. ACL is and was at all times during the Relevant Period, an APP entity within the meaning of s 6 of the *Privacy Act 1988* (Cth) (**Privacy Act**), requiring it (pursuant to s 15 of the Privacy Act) to not do an act, or engage in a practice, that breaches the Australian Privacy Principles (**APPs**), as contained in Schedule 1 to the Privacy Act.

10. In the course of the conduct of its business as a provider of healthcare services, ACL collected and held individual patients' personal and sensitive information, including health information for the purposes of providing test results and issuing invoices.

C. THE CYBERSECURITY RISKS FACING ACL DURING THE RELEVANT PERIOD

11. During the Relevant Period, ACL was operating in a high cyber threat landscape, with a significant cyber risk profile by reason of the fact that:

   a. ACL was a publicly listed company on the ASX and one of the largest private hospital pathology businesses in Australia, employing over 5,000 people and generating the revenue referred to in [7] above;

b. ACL was a business that used technology to deliver many of its services;

c. as part of providing its services to its customers, ACL routinely digitally handled and transferred large volumes of personal and sensitive information;

d. ACL was itself responsible for the creation, storage and use of sensitive information directly relating to individuals' health; and

e. ACL originates from the aggregation of multiple pathology businesses between 2015 and 2022, including Medlab Pathology Pty Ltd in December 2021, as described in [15] to [21] below.

12. During the Relevant Period, the cyber threat environment for businesses such as ACL was high and was documented as such. For example:

a. the United States based Health Information Sharing and Analysis Centre released a report in March 2022 detailing the growing sophistication and frequency of cyber threats targeting the healthcare sector globally at that time, highlighting the prevalence of ransomware attacks, phishing schemes, and supply chain vulnerabilities, as well as the challenges healthcare organisations faced at the time in securing sensitive patient data and maintaining operational continuity amongst these threats;

b. in the lead up to the Relevant Period, there had been a number of other businesses in the healthcare sector in the United States which had been targeted by cyber criminals, including as outlined in the 1H Healthcare Data Breach Report (August 2022) in the United States Health Insurance Portability and Accountability Act Journal;

c. the Australian Cyber Security Centre (**ACSC**) reported that, for the 2021-2022 financial year, the Health Care and Social Assistance sector reported the third highest number of cyber incidents (9%), behind State and Federal Government sectors;

d. in the Office of the Australian Information Commissioner's (**OAIC's**) publication titled 'Notifiable Data Breaches January 2021 – June 2021', it was reported that the health sector was the highest reporting industry sector, notifying 19% (85 notification) of all breaches, 56% of which were a result of a malicious or criminal attack, being the leading cause;

e. in the OAIC's publication titled 'Notifiable Data Breaches July 2021 – December 2021', the health sector was the highest reporting industry sector, notifying 18% (83 notifications) of all breaches, 47% of which were a result of a malicious or criminal attack, being the equal leading cause together with human error; and

f. in the OAIC's publication titled 'Notifiable Data Breaches January 2022 – July 2022', the health sector was the highest reporting industry sector, notifying 20% (79 notifications) of all breaches, 54% of which were a result of a malicious or criminal attack in all sectors, being the leading cause.

13. During the Relevant Period, unauthorised access to, or unauthorised disclosure of, personal information held by entities such as ACL gave rise to the risk of harm, including serious harm as that term is defined in the Privacy Act, to the individuals whose personal information those entities held, which included harm in the form of nuisance (where affected individuals would have been inconvenienced), financial harm (for example, the use of bank card or other personal information to incur debts to affected individuals) and personal harm (namely distress or psychological harm). Once an individual's personal information is disclosed on the dark web, it is not possible to recover it, meaning that there is a heightened and enduring risk of further exploitation, such as the possibility of future blackmail or identity theft. This may occur using personal information obtained through data breaches such as the Medlab Cyberattack (as defined in [22]), or by combining it with the growing body of leaked personal information from other data breaches. With the evolution of technology, these harms are ever evolving for individuals who have been the subject of a data breach. There is also a strong public interest in maintaining trust and confidence in the secure handling of personal information in the healthcare system. Incidents such as the Medlab Cyberattack create a serious risk of undermining this trust and confidence, which may impact on an individual's engagement with healthcare services.

14. During the Relevant Period, ACL was aware that the cyber threat environment it faced was high. As described in further detail in paragraph [34] below, in February 2021, ACL engaged StickmanCyber to consider ACL's cybersecurity posture and identify potential areas for improvement.

D. ACL'S ACQUISITION OF MEDLAB

15. On 19 December 2021, ACL acquired the assets of Medlab Pathology Pty Ltd (**Medlab**).

16. At the time of that acquisition, Medlab was a privately owned pathology business which provided and/or facilitated the provision of health services in New South Wales and Queensland, including prenatal genetic testing, fertility assessments and testing for sexually transmitted diseases. In the course of its business, Medlab collected and held individuals' personal information and sensitive information, which included health information, contact information, customer credit card information and payment details. It processed approximately 1.5 million pathology patient episodes per annum and held personal information and sensitive information relating to more than 223,000 individuals.

17. At the time of ACL's acquisition of Medlab, Medlab had two operating laboratories – one in Auburn, NSW and the other in Wilston, Queensland.

18. As part of its acquisition of Medlab, ACL acquired Medlab's computer and communications hardware, computer and information technology systems and equipment and software (**Medlab IT Systems**), such that on and from 19 December 2021, ACL owned and controlled the Medlab IT Systems. Further, on and from 19 December 2021, the IT team responsible for the day-to-day operations of the Medlab IT Systems reported to ACL's Chief Information Officer (**CIO**).

19. Prior to its acquisition of Medlab, ACL did not identify certain vulnerabilities in the Medlab IT Systems. The primary due diligence of the Medlab IT Systems and cybersecurity arrangements ACL had undertaken included a "Cybersecurity and Privacy Questionnaire". By Medlab's responses to this questionnaire, which ACL relied on as being true and accurate, ACL was aware that:

    a. Medlab had not conducted an IT penetration test, vulnerability assessment or IT security audit in the preceding three years;

    b. Medlab did not have sophisticated IT and cybersecurity processes in place, such as data recovery plans, and Medlab's IT and cybersecurity processes were less mature than those that ACL had in place at that time;

    c. to the best of its knowledge, Medlab had not been the subject of any cybersecurity incidents (including, but not limited to, IT breakdowns, failures or security breaches), including actual and attempted incidents;

d. to the best of its knowledge, Medlab had not been the subject of any complaints or investigations into any of its data collection and use by regulatory authorities, or by any industry groups to which it belonged; and

e. to the best of its knowledge, Medlab did not have any documents or reports prepared by or for it which identified threats to the security of personal or sensitive information handled by it.

20. In January 2022 (after the acquisition of Medlab), ACL put in place a plan to integrate (or, if integration was not appropriate, decommission) the Medlab IT Systems into ACL's core IT environment by 30 June 2022. That plan meant that the Medlab IT Systems would be kept separate from ACL's IT environment for a period of approximately six months while staff, equipment, laboratory testing and approved collection centres (meaning Medlab facilities where specimens are collected from patients for laboratory analysis) were integrated into ACL's environment. In January 2022, ACL established a steering committee to oversee and coordinate the integration, which included ACL's CIO, Chief Operating Officer, Chief Executive Officer, Chief Financial Officer, and other State Executive Officers and general managers.

21. In February 2022, following the preparation of a tailored "integration plan", the integration of the Medlab IT Systems commenced. The integration plan continued to be updated as the integration process progressed. By around 15 July 2022, the integration (or, if integration was not appropriate, the decommissioning) of Medlab's IT infrastructure had been substantially completed. In particular, by that time, Medlab's IT infrastructure from its main laboratories (in Auburn and Wilston) had either been integrated by ACL or decommissioned, apart from one datacentre containing 45 Medlab servers, which was integrated by early November 2022.

E. THE CYBERATTACK AND ACL'S RESPONSE TO IT

22. On or before 25 February 2022, a malicious actor known as the Quantum Group attacked part of the Medlab IT Systems, being the Medlab computer network which by that time was operated by ACL (**Medlab Cyberattack**). The events that led to ACL becoming aware of the Medlab Cyberattack and its response to the cyberattack are set out immediately below.

23. Between 4:04am and 5:18am on 25 February 2022, the [redacted] Antivirus software running on the servers within the Medlab IT Systems detected 51 servers with the presence of QuantumLocker malware.

24. At 5:04am on 25 February 2022, the [redacted] Antivirus logs indicated that two Domain Controllers used by Medlab had been compromised with QuantumLocker malware. Domain Controllers are a central component for enterprises running Windows systems, which provide a central method of authentication and management of systems across an enterprise.

25. An employee of ACL first became aware of the Cyberattack at around 5:00am on 25 February 2022 when he attempted to log-in to a computer on the Medlab network. He noticed new icons on the desktop display, including a Google Chrome icon which said: "Read Me". He clicked on the icon and was presented with a ransomware demand from the Quantum Group (**Demand**) which stated (relevantly):

> *"During the period your network was under our control, we downloaded a huge volume of information... This information contains a lot of sensitive, private and personal data... Publishing of such data will cause serious consequences and even business disruption... After a payment you'll get network decryption, full destruction of downloaded data... If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site... ".*

26. After he read the Demand, at around 5:15am on 25 February 2022, the employee of ACL referred to in [25] above notified an IT Helpdesk and Support Member of Medlab's IT team of the Demand.

27. At 6:05am on 25 February 2022, Medlab's IT Support Team comprising six personnel employed by ACL at the time were made aware, through an automated email alert, that 10 Medlab computers, running [redacted] Antivirus software, had recent threats that required investigation.

28. By 9:00am on 25 February 2022, other employees of ACL had identified that the Demand had appeared on their computers and that files on those computers had been modified to have the ".quantum" extension added to their file names.

29. At 9:51am on 25 February 2022, the following personnel employed by ACL were informed by R-IT Solutions (an external provider to ACL that monitored its IT systems) that ransomware had been detected on three Medlab servers:

a. Chief Operations Officer, Medlab;

b. IT Team Leader and Application Support, Medlab; and

c. IT Network and System Support, Medlab.

30. The three servers on which the ransomware was detected were:

a. the server known as [redacted], being a file server within Medlab's IT Systems used for holding all user profile files;

b. the server known as [redacted] was used as Medlab's Laboratory Information System which processed, stored and managed patient data for clinical laboratories; and

c. the server known as [redacted], which was a [redacted] server in Medlab's network, that was used for creating and distributing some of Medlab's reports.

31. At 10:22am on 25 February 2022, a member of the IT Team, Helpdesk and Support for Medlab acknowledged a message from the employee of ACL who first became aware of the Cyberattack and requested that that employee forward him a copy of the Demand.

32. At about 12:45pm and 12:49pm on 25 February 2022, ACL's Head of Technical Services provided the Medlab IT Team Leader and Application Support with the following playbooks:

a. Malware outbreak playbook – dated August 2021; and

b. Ransomware playbook – dated August 2021.

33. Prior to being provided the Ransomware and Malware Outbreak playbooks on 25 February 2022, the Medlab IT Team Leader and Application Support had not seen or used these playbooks or received training on them.

34. At around 1:32pm on 25 February 2022, ACL instructed StickmanCyber (an external cybersecurity firm) to investigate, respond to, and to provide advice in relation to the Medlab Cyberattack. Since February 2021, StickmanCyber had been engaged by ACL to provide services in relation to ACL's IT environment more generally including to conduct a review of ACL's cybersecurity processes and controls in 2021 for the purposes of getting a better understanding of ACL's cybersecurity posture and capabilities, to identify any control weaknesses, and to design a program of works to

uplift ACL's cybersecurity settings (prior to ACL's acquisition of Medlab). StickmanCyber's engagement was later formally reflected in a Master Services Agreement with Clinical Labs, which was signed by StickmanCyber on 25 February 2022 and Clinical Labs on 2 March 2022 respectively (**StickmanCyber MSA**). Pursuant to the StickmanCyber MSA, StickmanCyber and Clinical Labs executed 'Service Order No. 1', which was signed by StickmanCyber on 25 February 2022 and Clinical Labs on 2 March 2022 respectively (**Service Order No. 1**).

35. StickmanCyber remained involved in the response to the Medlab Cyberattack until 1 March 2022, spending 44.5 hours on the engagement. During that time, StickmanCyber:

    a. deployed monitoring agents on three of the at least 127 computers affected by the Cyberattack;

    b. examined the backed-up firewall logs, although only one hour of data was available for analysis;

    c. performed periodic searches of the dark web between 25 February 2022 and 1 March 2022; and

    d. concluded that the attack vector was delivered through a macro or email addressed to the employee who had alerted IT staff for Medlab to the Medlab Cyberattack. Stickman Cyber conducted a limited investigation of whether the Quantum Group may have established persistence mechanisms to stay connected to the Medlab IT Systems and its network (as described in further detail in [42] below).

36. By 2:35pm on 25 February 2022, StickmanCyber confirmed that computers and servers had the presence of QuantumLocker malware (being the file with the filename "TTSEL.exe").

37. By 7:00pm on 25 February 2022, StickmanCyber had identified the malware file responsible for encrypting or attempting to encrypt certain computers and servers in the Medlab IT environment. By that time, StickmanCyber was also aware that the [redacted] Antivirus software logs showed that 51 systems (all running [redacted] Antivirus software) had detected the QuantumLocker malware (as referred to in [23] above). One of those systems was the "Auburn LAN Network Server" referred to further in [62(b)] below.

38. The [redacted] Antivirus software logs also showed that the threat actor who deployed the "QuantumLocker" malware within those systems was able to successfully access them with an "Administrator" account (being the highest user permission level granted on a Windows computer system).

39. At 10:48pm on 25 February 2022, StickmanCyber informed ACL that (relevantly):

> "*We are at a point where we feel fairly sure that we are on top of the incident.*
>
> *We see that the executable only fired once across the network, potentially from a Doctor's machine this morning. His machine has been scanned with* [redacted] *and the file that is deemed to have caused the incident, is still to be verified by the Medlab team as quarantined on that machine.*
>
> ...
>
> *The ransom note has stated that in 48 hours they will post your data on site, ETC. 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…*".

40. By 26 February 2022, the IT Team Leader and Application Support for Medlab was made aware that a further 59 computers (53 workstations (PCs) and 6 laptops) had detected the QuantumLocker malware. Those devices were protected with an antivirus product known as [redacted]

41. At 12:41pm on 27 February 2022, StickmanCyber informed ACL (relevantly):

    a. that the malware file was responsible for encrypting or attempting to encrypt systems, which had the filename "TTSEL.exe";

    b. that the logs from those systems utilising [redacted] Antivirus (51 systems) showed that all the systems running [redacted] Antivirus detected the malware;

    c. that the logs from those systems utilising [redacted] Antivirus (51 systems) showed the user account logged onto the system at the time of the detection, being the "Administrator" account (being the highest user permission level granted on a Windows computer system); and

    d. of the type of data held within the three servers affected by the malware (as described in [30] above).

42. StickmanCyber conducted a limited investigation of whether the threat actor (the Quantum Group) may have established mechanisms to stay connected to the Medlab IT Systems and its network. After having taken the steps described in [35] above, on 1 March 2022, StickmanCyber ceased investigating whether there had been any exfiltration of data as a result of the Medlab Cyberattack, with the last dark web scan being conducted on that day.

43. On 2 March 2022, ACL was provided with StickmanCyber's findings and conclusions as set out in its "Incident Summary Report". In the section of that report entitled "Root Cause", StickmanCyber stated (relevantly):

> *"What we know so far:*
>
> *Root Cause A doctor's PC was infected and TSsel.exe was executed. Ttsel.exe executed in 2 parts. First it spread worm-like across the network and added attribute .quantum to all readable files. It then ran an execution to encrypt all .quantum files. The PCs with* [redacted]*, with no exceptions, detected the executable and quarantined it. Any PCs with* [redacted] *also quarantined the executable. Any machines with* [redacted] *were vulnerable. It is assumed that the Firewall* [redacted] *IPS was not able to prevent the infection as the exploit was either delivered through a macro or email."*

44. On 11 March 2022, StickmanCyber closed its investigation.

45. On 15 March 2022, the Head of Technical Services at ACL received an email from StickmanCyber concerning the notifiable data breach scheme in the Privacy Act and provided a link to the website of the Office of the Australian Information Commissioner concerning that scheme. In that email, StickmanCyber stated (relevantly):

> *"From my perspective, and this is just my perspective, [the notifiable data breach regime] concerns itself with a breach where personal identifiable information is lost/stolen/deleted etc.*
>
> *The important part of that site to read is: Identifying eligible data breaches: Questions to ask:*
>
> 1. *Is the breach likely to result in serious harm to any individuals? From what we saw, no data was exfiltrated from the business, instead there was a worm that spread an encryption exe throughout the network.*

2. *Did the entity act quickly to delay and remediate the data breach, avoiding serious harm to an individual? I would say yes, the medlabs [sic] team set out to try to remediate the breach immediately and you engaged an incident response team to help with the identification and remediation.*

...

But at the end of the day, this all goes back to the question, did the breach cause harm to any individuals?

At the point where we ended our engagement, I would have to say no."

46. By 18 March 2022, ACL's CIO and Head of Technical Services formed the view that the threat posed by the Medlab Cyberattack had been contained and that there was no information which suggested that personal information held by the Medlab IT Systems had been exfiltrated.

47. By 21 March 2022, based on the analysis conducted, and advice provided, by StickmanCyber by that time, ACL had determined that the Medlab Cyberattack was not an eligible data breach within the meaning of s 26WE of the Privacy Act.

48. At 5:28am on 25 March 2022, the ACSC notified ACL that the ACSC had received intelligence from a trusted third party that Medlab may be the victim of a ransomware incident and reminded ACL that it may be required to notify the Commissioner and affected individuals (**first ACSC notification**). That email stated (relevantly):

"We are reaching out to notify you that we have received intelligence from a trusted third party that Melab Pathology may be the victim of a ransomware incident.

...

Please note we have not independently verified this information but are providing it to you for your awareness.

We would appreciate it if you could forward this email to the relevant IT team for assessment.

If possible, can you please confirm if you have been compromised? And, if so, can you please answer the below questions...

...

If a data breach involving personal information has resulted from this incident, you may be required to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals."

49. At 3:10pm on 25 March 2022, ACL's CIO sent an email to the ACSC with details of the Medlab Cyberattack and informed the ACSC that, following monitoring of impacted devices and the dark web, ACL did not believe that any data had been exfiltrated.

50. On 29 March 2022, ACL's CIO provided an update to the ACL Board about the Medlab Cyberattack. That update stated (relevantly):

> *"On the 25th February, the IT team at Auburn detected suspicious activity on a PC after a user was unable to log in, Malware and ransomware were soon discovered on numerous devices. It appears this got into the organisation by the action of a Pathologist clicking on a malicious link in an email. Stickman Cyber was engaged to manage this incident. Following monitoring of two infected machines over 72hrs, no exfiltration of data was detected out of the network. At this point, we have no reason to believe any [personal health information] or company data was breached.*
>
> *The attack was limited to devices running the* [redacted] *Antivirus software or older non-critical or non-production window servers which were unable to detect and neutralise the malware. Current production servers were using* [redacted] *Antivirus software which was able to protect those devices. As such the lab was able to continue to operate throughout the incident as the team methodically worked through cleaning and installing* [redacted] *on desktops and laptops.*
>
> *CIO review[ed] the impact of this incident against the LIS upgrade go-live activities occurring the following day. Go-live approval was given as it was limited to Medlab and no evidence was found within the wider group and was closely monitoring through the Friday.*
>
> *We have reached the final phase for this incident being "Follow-up". All identification, containment, eradication and recover phases have been completed as per the timeline on the next slide."*

51. Contrary to what was stated by StickmanCyber in its "Incident Summary Report", the conclusions of ACL's CIO and Head of Technical Services which were based on the advice provided by StickmanCyber (as set out in [43] and [45] above), as well as the CIO's update to the Board of 29 March 2022, data was in fact exfiltrated from certain servers in the Medlab IT environment as a result of the Medlab Cyberattack. In particular, the Quantum Group exfiltrated 86 gigabytes of data, at least some of which comprised personal information and sensitive information under s 6 of the Privacy Act, including passport numbers, health information and financial information. On or before 16 June 2022, the exfiltrated information was published on the dark web.

52. At 10:26am on 16 June 2022, the ACSC sent ACL a second notification (**second ACSC notification**), which stated (relevantly):

> "*The [ACSC] has received a report from a trusted third party regarding a potential data breach impacting [Medlab]. Through monitoring of dark web sources, it has come to our attention that potentially 80gb of Medlab data was published from the Quantum group. Initial investigation by the third party has shown that Personal Identifiable Information (PII), Protected Health Information (PHI), and financial information is available including credit card details with names, card numbers, expiry and ccv, although the ACSC has not verified this*".

53. Following the second ACSC notification, ACL started taking internal and external legal advice, including from Clyde & Co.

54. At 2:53pm on 16 June 2022, ACL's Head of Technical Services sent an email to individuals at ACL, Medlab and StickmanCyber which said that he was satisfied that:

    a. data had been exfiltrated from its systems containing complete credit card information and personal health information;

    b. the exfiltrated data was related to the Medlab Cyberattack;

    c. the data was publicly visible on the dark web;

    d. it was likely that it was obligated to notify the Commissioner and would potentially need to advise all individuals affected that their data had been stored and compromised.

55. Between 22 June 2022 and 10 July 2022, Clyde & Co, at the direction of ACL, accessed and conducted an initial review of the Medlab data which had been exfiltrated and published by the Quantum Group. In that time, ACL did not receive any new information about the exfiltrated data beyond that already known to ACL on 16 June 2022.

56. On 10 July 2022, ACL provided a statement under s 26WK of the Privacy Act to the Commissioner, informing her that ACL had reasonable grounds to believe that the Medlab Cyberattack amounted to an "eligible data breach" in respect of the Medlab systems (within the meaning of s 26WE of the Privacy Act). That statement provided (relevantly):

> *"On 16 June 2022, the Australian Cyber Security Centre (ACSC) notified Medlab of an unverified report regarding a potential data breach carried out by the Quantum group, a known ransomware threat actor (Notice). The Notice provided a link to the Quantum blog referencing the potential breach and from which the data had been published on the dark web. At the time of receiving the Notice, Medlab was unaware of the potential data breach, however, Medlab was aware that an incident had occurred on or around 25 February 2022 involving potential unauthorised access to Medlab's network.*
>
> *Upon becoming aware of the incident at that time, Medlab immediately commissioned an independent forensic investigation into the incident and carried out all remedial action recommended by the cyber security provider it had commissioned. Based on the investigation and monitoring conducted in February, Medlab determined that the incident was not an eligible data breach requiring notification, as there was no conclusive information or evidence available at the time to suggest that any personal information had been exfiltrated or accessed. Following monitoring of two infected machines over 72 hours which were isolated, firewall and server audit logs were examined, and no exfiltration of data was detected out of the Medlab network. Dark web scans were also conducted at the time for evidence of any data exfiltration and no traces were detected. Medlab now suspects the potential breach referred to in the Notice is related to the incident that was investigated in February.*

> *On receiving the Notice, Medlab immediately engaged cyber security experts to conduct an assessment and investigate the suspected breach. The forensic investigation and analysis of the data to determine the individuals who may be potentially affected by the breach is still ongoing. The experts do not currently have a precise view on when this investigation may conclude, however, anticipate further clarity on this point in the next 2 weeks. The files and data that have been exposed by the Quantum group on the dark web have been difficult to access and download by Medlab's security experts in order to carry out a thorough forensic investigation and, therefore, it is taking some time to do that. Once the cyber security investigation is completed, Medlab will take appropriate steps to update the OAIC and notify any potentially affected individuals in accordance with 26WL(2) of the Privacy Act 1988 (0th) (Privacy Act)."*

57. The statement also identified that the following kinds of personal information and sensitive information held on the Medlab systems were potentially involved in the Cyberattack: financial details, tax file numbers, identity information, contact information and health information (as defined under s 6FA of the Privacy Act).

58. On 27 October 2022, ACL made an ASX announcement and published the announcement on ACL's website relating to the Medlab Cyberattack. That ASX notice stated (relevantly):

> *"ACL has conducted a forensic analysis of the affected information and has determined that personal information of approximately 223,000 individuals has been affected, with information accessed of different levels of concern. This group of individuals is largely confined to NSW and Queensland.*
>
> *A summary of the records breached of most concern are:*
>
> - *~17,539 individual medical and health records associated with a pathology test;*
> - *~28,286 credit card numbers and individuals' names. Of these records, ~15,724 have expired and ~3,375 have a CVV code; and*
> - *~128,608 Medicare numbers (not copies of cards) and an individual's name.*

...

ACL, on behalf of Medlab, will commence the process of directly contacting at risk individuals by email and postal mail today, to provide them with information about the incident, how it affects them and additional steps that can be taken to protect their information. Detailed information about the incident has also been made available on Medlab and ACL websites providing an information source and a proactive way to contact the company for those who are at all concerned.

ACL has established a dedicated inbound response team to answer questions from notified individuals and provide them with guidance and remediation advice in relation to the incident. ACL has also established a 'care team' for those whose health information records may have been affected, to minimise distress and provide necessary support.

ACL will be offering free-of-charge credit monitoring and/or ID document replacement to individuals whose affected information types may put them at risk of credit and/or identity fraud, and is working alongside Federal and State government authorities in this regard.

ACL Chief Executive Officer Melinda McGrath said: "On behalf of Medlab, we apologise sincerely and deeply regret that this incident occurred. We recognise the concern and inconvenience this incident may cause those who have used Medlab's services and have taken steps to identify individuals affected. We are in the process of providing tailored notifications to the individuals involved. We want to assure all individuals involved that ACL is committed to providing every reasonable support to them. We will continue to work with the relevant authorities."

59. On 19 October 2023, the ACSC informed ACL that it had received a report from a third-party regarding data from ACL being listed for sale on the dark web (**Dark Web Post**).

60. Following being informed of the Dark Web Post, ACL conducted an investigation which involved:

    a. reviewing ACL's environment for any signs of compromise;

b. engaging the specialist Digital Forensics and Incident Response team at McGrath Nicol to conduct a forensic investigation, the outcome of which was that there was no indication of unauthorised network exfiltration or compromise and that it was unlikely that the data referred to in the ACSC's report was related to any recent compromise of ACL's environment;

c. commencing active monitoring of the dark web for indicators of unauthorised activity, which was not identified; and

d. comparing the Dark Web Post to previous posts on the dark web relating to data exfiltration during the Medlab Cyberattack, the result of which was that similarities to a previous post in August 2022 were identified.

61. As a result of that investigation and based on the advice provided by McGrath Nicol, ACL concluded that the Dark Web Post was most likely a re-post of the data exfiltrated during the course of the Medlab Cyberattack and that there had been no further exfiltration of data.

F. DEFICIENCIES IN THE MEDLAB IT SYSTEMS

62. The personal information that was exfiltrated during the Medlab Cyberattack was held on two categories of the Medlab IT Systems:

a. computers used in the Wilston and Auburn laboratories of Medlab; and

b. the primary file server known as the "Auburn LAN Network Server".

63. Throughout the Relevant Period, and before they were integrated with ACL's core IT environment, the computers used by Medlab:

a. deployed [redacted] Antivirus software, which was not capable of preventing the particular malicious files used by the Quantum Group as part of the Medlab Cyberattack from being written or run on those systems;

b. deployed weak authentication measures and did not require users to use multifactor identification (**MFA**) to utilise the Medlab VPN. MFA is a security enhancement that requires users of IT systems to provide more than one form of identification to access an account or system. Without MFA, a threat actor likely would be able to reuse any stolen credentials;

c. had installed on them only the default email protection provided by "Office 365", which was simple for threat actors to bypass;

d. were subject to firewalls which only had the capacity to log one hour of activity before that log was deleted;

e. were used in Medlab collection centres that had basic network perimeter protection and connected directly to the internet, which meant that the computers had limited protection from threat actors who accessed the Internet from those computers; and

f. did not include any form of file encryption to protect data stored on them.

64. Throughout the Relevant Period, and before it was integrated into ACL's core IT network, Medlab's "Auburn LAN Network Server":

a. was running a legacy version of a Windows Server that did not receive mainstream support from Microsoft, patches for vulnerabilities, or enhanced security protections, from 14 January 2020; and

b. deployed [redacted] Antivirus software, which did not prevent or detect a threat actor uploading data from the server to the Internet.

65. The deficiencies described in [63] and [64] above are together hereafter referred to as the **Medlab IT Systems Deficiencies**.

G. DEFICIENCIES IN THE RESPONSE TO THE MEDLAB CYBERATTACK

66. At the time of the Medlab Cyberattack, the response to the Medlab Cyberattack was deficient in the following respects:

a. the playbooks used to respond to cyber incidents, including those which were provided to the Medlab IT Team Leader (as described in [32] above):

i. contained generalised steps for responding to cyber incidents;

ii. did not clearly define roles and responsibilities for incident response efforts;

iii. contained limited detail on containment processes that should be deployed in the event of a cyber incident;

iv. provided limited detail on steps that should have been taken to mitigate exfiltration of data in the event of a cyber incident; and

v. recommended steps for technologies not used within the Medlab IT Systems;

b. incident management processes had not been adequately tested during the two-month period between when ACL completed its acquisition of Medlab and the date of the Medlab Cyberattack, with only a tabletop exercise having been conducted (and which did not include any of the Medlab personnel, employed by ACL, involved in the response to the Medlab Cyberattack as described in [29] above);

c. 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;

d. Medlab was not using adequate endpoint and response tooling/products that could perform behavioural-based analysis of activities on the Medlab IT Systems to determine if they exhibited malicious actions that might be otherwise undetected by any antivirus product;

e. Medlab did not have any application whitelisting in place to prevent unknown or unauthorised applications from running on them and only deployed [redacted] Antivirus on Medlab computers. Without application whitelisting and relying only on antivirus software, a threat actor would likely have been able to use its own malicious tools, provided they were not commonly known, as they would not be detected and prevented by the [redacted] Antivirus software;

f. there were limited communication plans outlining lines of communication with internal and external stakeholders, including communication with executive management teams, regulators, the media and individuals whose personal information may have been compromised by the cyber incident;

g. as described in [33] above, the Medlab IT Team Leader who was initially tasked with managing the Medlab Cyberattack had not seen, used or received training on the playbooks provided to her, and had no formal cybersecurity background or incident response training;

h. the Medlab IT Systems had limited security monitoring capability in that firewall logs on the Medlab network were only retained for one hour. The Medlab IT Systems also had limited incident notification capability;

i. specific data recovery plans for the Medlab IT Systems had not been developed; and

j. [redacted]. Medlab staff were not required to use MFA to use the Medlab VPN.

67. The deficiencies described in [66] above are hereafter referred to as the **Medlab Cyberattack Response Deficiencies**.

H. CONTRAVENTIONS OF THE PRIVACY ACT

68. During the Relevant Period, under s 13(1)(a) of the Privacy Act, an act or practice of an APP entity is an interference with the privacy of an individual if the act or practice breaches an APP in relation to personal information about the individual.

69. During the Relevant Period, under s 13(4A) of the Privacy Act, if an APP entity contravened, relevantly ss 26WH(2) and 26WK(2) of the Privacy Act, the contravention was taken to be an act that is an interference with the privacy of an individual.

70. During the Relevant Period, an APP entity contravened s 13G(a) of the Privacy Act if the entity did an act, or engaged in a practice, that was a serious interference with the privacy of an individual. Each contravention of s 13G(a) of the Privacy Act attracted a maximum civil penalty of $2,200,000.

Breach of APP 11.1(b) and resultant contraventions of s 13G(a) of the Privacy Act

71. Under APP 11.1(b), ACL was required to take such steps as were reasonable in the circumstances to protect the personal information ACL held from unauthorised access or disclosure.

72. Having regard to:

a. the nature and size of ACL's business, as described in [7] and [8] above;

b. the nature and volume of the personal information, including sensitive information, held on the Medlab IT Systems as described in [16] above;

c. the high cybersecurity risks facing ACL during the Relevant Period, and the risk of serious harm to individuals whose personal and sensitive information (including health information) was held on the Medlab IT Systems if that information was subject to unauthorised access and/or disclosure;

d. the limited due diligence conducted by ACL into the Medlab IT Systems prior to ACL's acquisition of Medlab;

e. ACL's lack of a complete understanding of the Medlab IT Systems upon ACL's acquisition of Medlab as referred to in [19] above;

f. the Medlab IT Systems Deficiencies; and

g. the Medlab Cyberattack Response Deficiencies,

during the Relevant Period, ACL did not have in place adequate cybersecurity controls in respect of Medlab, which meant that it did not take such steps as were reasonable to protect the personal information ACL held on the Medlab IT Systems from unauthorised access or disclosure.

73. By reason of the matters referred to in [72] above, during the Relevant Period, ACL breached APP 11.1(b) of the Privacy Act.

74. The breach of APP 11.1(b) referred to in [73] above in respect of the management of the Medlab IT Systems was an interference with the privacy of more than 223,000 individuals whose personal information ACL held on the Medlab IT Systems for the purposes of the Privacy Act.

75. That breach of APP 11.1(b), and resultant interference with the privacy of more than 223,000 individuals referred to in [74] above, was serious, including because of:

a. the circumstances referred to in [72(a)] to [72(e)] above;

b. the fact that the risk of unauthorised access and disclosure was realised when, by reason of the Medlab Cyberattack the Quantum Group exfiltrated 86 gigabytes of data held on the Medlab IT Systems, at least some of which comprised personal information and sensitive information under s 6 of the Privacy Act, including passport numbers, health information and financial information, and was published on the dark web, as described in [51] above; and

c. the fact that the exfiltrated data was the subject of the Dark Web Post.

76. By reason of the matters described in [62] to [75] above, ACL engaged in a separate contravention of s 13G(a) of the Privacy Act in respect of each of the more than 223,000 individuals whose personal information was held on the Medlab IT Systems throughout the Relevant Period.

Breach of s 26WH(2) and resultant contravention of s 13G(a) of the Privacy Act

77. During the Relevant Period, s 26WE of the Privacy Act applied if, relevantly both: (i) an APP entity held personal information relating to one or more individuals; and (ii) the APP entity was required under s 15 of the Privacy Act not to do an act, or engage in a practice, that breaches APP 11.1 in relation to that personal information.

78. During the Relevant Period, under s 26WE(2) of the Act:

a. if:

i. there was unauthorised access to, or unauthorised disclosure of, the information; and

ii. a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates,

then:

b. the access or disclosure covered by paragraph (a) was an **eligible data breach** of the APP entity; and

c. an individual covered by subparagraph (a)(ii) was **at risk** from the eligible data breach.

79. Section 26WH applied to ACL during the Relevant Period. During the Relevant Period, s 26WH of the Privacy Act applied if:

a. an entity was aware that there were reasonable grounds to suspect that there may have been an eligible data breach of the entity; and

b. the entity was not aware that there were reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity.

80. Under s 26WH(2) of the Privacy Act, upon becoming aware that there were reasonable grounds to suspect that there may have been an eligible data breach (as defined in s 26WH(2) and referred to in [78] above), an APP entity was required to:

    a. carry out a reasonable and expeditious assessment of whether there were reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and

    b. take all reasonable steps to ensure that the assessment was completed within 30 days after the entity was aware that there were reasonable grounds to suspect that there may have been an eligible data breach of the entity.

81. By 2 March 2022, by reason of the circumstances described in [23]-[43] above, ACL:

    a. was aware that there were reasonable grounds to suspect that there may have been an eligible data breach in respect of the Medlab systems; and

    b. was not aware that there were reasonable grounds to believe that those circumstances amounted to an eligible data breach in respect of the Medlab systems.

82. In particular, the circumstances described in [23]-[43] above supplied reasonable grounds for ACL to suspect by 2 March 2022 that:

    a. there had been unauthorised access to the personal information of individual customers and patients that was held on the Medlab IT Systems, which were controlled by ACL at that time; and

    b. that access would be likely to result in serious harm to any of the over 223,000 individuals to whom the information related, which harm included that described in [13] above.

83. By reason of the matters referred to in [81] and [82] above, under s 26WH(2) of the Privacy Act, ACL was required to carry out a reasonable and expeditious assessment of whether there were reasonable grounds to believe that the circumstances described in [23]-[43] above in relation to Medlab amounted to an eligible data breach of ACL, and to take all reasonable steps to ensure that the assessment was completed within 30 days of 2 March 2022.

84. ACL did not carry out a reasonable and expeditious assessment of whether there were reasonable grounds to believe that the circumstances described in [23]-[43] above amounted to an eligible data breach in respect of Medlab. In particular:

a. the assessment undertaken by StickmanCyber (as described in [35]-[43] above) was inadequate, and therefore not reasonable, because:

i. StickmanCyber only deployed monitoring agency on 3 of the at least 127 computers subject to the QuantumLocker ransomware deployed by the threat actor;

ii. StickmanCyber did not conduct an investigation into the threat actor and its attack traits, to determine whether data was likely to have been exfiltrated;

iii. StickmanCyber's assessment of the Medlab Cyberattack was based on a review of only one hour of firewall logs, which it did not access until approximately four hours after the Demand was first downloaded; and

iv. StickmanCyber conducted a limited investigation of whether the threat actor (the Quantum Group) may have established persistence mechanisms to stay connected to the Medlab IT Systems and its network; and

b. ACL was aware that StickmanCyber's assessment was limited in the ways described in subparagraph (a) above, and therefore it was unreasonable for ACL to rely solely on the investigation conducted by StickmanCyber and StickmanCyber's advice referred to in [45] above to conclude by 21 March 2022 that the threat posed by the Medlab Cyberattack had been contained and that there was no information which suggested that personal information held by the Medlab IT Systems had been exfiltrated.

85. By reason of the matters referred to in [84] above, ACL breached s 26WH(2) of the Privacy Act.

86. Under s 13(4A) of the Privacy Act, ACL's breach of s 26WH(2) of the Privacy Act is taken to be an interference with the privacy of an individual.

87. ACL's breach of s 26WH(2) of the Privacy Act was serious, including because of:

a. the nature and volume of the personal information, including sensitive information, held on the Medlab IT Systems the subject of the Medlab Cyberattack as described in [16] above;

b. the high cybersecurity risks facing ACL during the Relevant Period, and the risk of serious harm to individuals whose personal information was held on the Medlab IT Systems if that information was subject to unauthorised access and/or disclosure, and ACL's knowledge of those matters, as described in [11]-[14] above;

c. the fact that the failure to conduct the reasonable and expeditious assessment resulted in an incorrect conclusion by ACL by 21 March 2022 that there were not reasonable grounds to believe that eligible data breach had occurred in respect of Medlab; and

d. the fact that the failure to conduct the reasonable and expeditious assessment resulted in a delay in ACL notifying the Commissioner that there were reasonable grounds to believe that there had been an eligible data breach of ACL (which did not occur until 10 July 2022, as described in [56] above) and accordingly delaying the Commissioner's ability to monitor ACL's notification of those individuals whose personal information may have been compromised as a result of the Cyberattack which did not occur until 27 October 2022, as described in [58] above.

88. By reason of the matters described in [69], [70] and [77]-[87] above, ACL engaged in a single contravention of s 13G(a) of the Privacy Act.

Breach of s 26WK and resultant contravention of s 13G(a) of the Privacy Act

89. During the Relevant Period, ss 26WK(1) and (2) of the Privacy Act provided that if an entity was aware that there were reasonable grounds to believe that there had been an eligible data breach of the entity, the entity was required to prepare a statement that complied with s 26WK(3) of the Privacy Act and give a copy of that statement to the Commissioner as soon as practicable after the entity became so aware.

90. By at least 16 June 2022, following the second ACSC notification, ACL was aware that there were reasonable grounds to believe that there had been an eligible data breach in respect of Medlab. It was practicable for ACL to prepare a statement that complied with s 26WK(3) of the Privacy Act and give a copy of that statement to the Commissioner

within two to three days thereafter. ACL failed to do so and did not provide such a statement to the Commissioner until 10 July 2022.

91. By reason of the matters referred to in [90] above, ACL breached s 26WK(2) of the Privacy Act.

92. Under s 13(4A) of the Privacy Act, ACL's breach of s 26WK(2) of the Privacy Act is taken to be an interference with the privacy of an individual.

93. ACL's breach of s 26WH(2) of the Privacy Act was serious, including because of:

    a. the nature and volume of the personal information, including sensitive information, held on the Medlab IT Systems the subject of the Medlab Cyberattack as described in [16] above;

    b. the high cybersecurity risks facing ACL during the Relevant Period, and the risk of serious harm to individuals whose personal information was held on the Medlab IT Systems if that information was subject to unauthorised access and/or disclosure, and ACL's knowledge of those matters, as described in [11]-[14] above; and

    c. the fact that its delay in providing a statement that complied with s 26WK(3) of the Privacy Act to the Commissioner delayed her ability to perform her statutory functions, which included:

        i. monitoring ACL's notification to those individuals whose personal information may have been compromised as a result of the Medlab Cyberattack which did not occur until 27 October 2022, as described in [59] above;

        ii. providing guidance and education to the community about the impact of the Medlab Cyberattack; and

        iii. engaging with other relevant Government agencies.

94. By reason of the matters described in [69], [70] and [89]-[93] above, ACL engaged in a single contravention of s 13G(a) of the Privacy Act.

I. FACTS AND CIRCUMSTANCES RELEVANT TO PECUNIARY PENALTIES

95. Under s 80U(1) of the Privacy Act, the civil penalty provisions of the Privacy Act (including s 13G(a) of the Privacy Act as in force during the Relevant Period) are

enforceable under Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (**Regulatory Powers Act**).

96. Under s 80U(2) of the Privacy Act, for the purposes of Part 4 of the Regulatory Powers Act, the Commissioner is an authorised applicant in relation to the civil penalty provisions of the Privacy Act (including s 13G(a) of the Privacy Act). Accordingly, under s 82(1) of the Regulatory Powers Act, the Commissioner is entitled to apply to the Federal Court for an order that ACL pay the Commonwealth pecuniary penalties for its contraventions of s 13G(a) of the Privacy Act it has admitted in this SAFA.

97. Under s 82(3) of the Regulatory Powers Act, if the Court is satisfied that ACL has contravened s 13G(a) of the Privacy Act (as admitted in this SAFA), the Court may order ACL pay to the Commonwealth such pecuniary penalty for the contraventions as the Court determines to be appropriate. Under s 82(5)(a) of the Regulatory Powers Act, for a body corporate such as ACL, the pecuniary penalty must not be more than five times the pecuniary penalty specified for the civil penalty provision. A contravention of s 13G(a) during the Relevant Period attracted a maximum civil penalty of 2,000 penalty units, which during the Relevant Period, was $220. Accordingly, the maximum penalty for each contravention of s 13G(a) during the Relevant Period was $2,200,000 per contravention.

98. Under s 82(6) of the Regulatory Powers Act, in determining the pecuniary penalty, the Court must take into account all relevant matters, including:

    a. the nature and extent of the contravention;

    b. the nature and extent of any loss or damage suffered because of the contravention;

    c. the circumstances in which the contravention took place;

    d. whether the person has previously been found by a court (including a court in a foreign country) to have engaged in any similar conduct.

Nature and extent of the contraventions (s 82(6)(a) of the Regulatory Powers Act) and the circumstances of the contraventions (s 82(6)(c) of the Regulatory Powers Act)

99. The contraventions of s 13G(a) of the Privacy Act admitted by ACL all relate to its ability during the Relevant Period to manage and respond to the cybersecurity risks associated with the Medlab IT systems, which were under ACL's control throughout

the whole of the Relevant Period. While the Medlab IT Systems were only acquired by ACL at the beginning of the Relevant Period, they were immature in terms of their cybersecurity controls and therefore significantly more exposed to the risk of a cyberattack during the six-month period it took ACL to integrate them into ACL's core IT environment. ACL was aware of that risk. That risk materialised in the Medlab Cyberattack which led to the exfiltration of 86 gigabytes of data, at least some of which comprised personal information and sensitive information under s 6 of the Privacy Act, including passport numbers, health information and financial information. On or before 16 June 2022, the exfiltrated information was published on the dark web.

100. The s 13G(a) contraventions that occurred by reason of ACL's breach of APP 11.1(b):

a. totalled at least 223,000 contraventions, with there being a separate serious interference with the privacy of the approximately 223,000 individuals whose personal information was held by ACL on the Medlab IT Systems; and

b. occurred across the whole of the Relevant Period.

101. The s 13G(a) contraventions that occurred by reason of ACL's breaches of ss 26WH and 26WK of the Privacy Act:

a. totalled two contraventions (a single contravention in respect of the breach of s 26WH and a single contravention in respect of the breach of s 26WK); and

b. occurred following the Medlab Cyberattack and in the context of ACL's response to it.

The nature and extent of any loss or damage suffered because of the contraventions

102. ACL's contraventions of s 13G(a) of the Privacy Act that occurred by reason of ACL's breach of APP 11.1(b) exposed the personal information of a significant number of individuals (including sensitive health information) to the risk of misuse and public disclosure. That risk materialised when the Medlab business owned by ACL was the subject of the Medlab Cyberattack exposing approximately 223,000 individuals to potential emotional distress and the material risk of identity theft, extortion and financial crime. That risk further materialised when the data exfiltrated during the Medlab Cyberattack was "reposted" through the Dark Web Post.

103. There is accordingly a reasonable inference available that the contraventions of s 13G(a) of the Privacy Act that occurred by reason of ACL's breach of APP 11.1(b)

had the potential to result in loss and damage to some of the individuals whose personal information was held by ACL on the Medlab IT Systems impacted by the Medlab Cyberattack, particularly those individuals whose personal information was exfiltrated and disclosed on the dark web. ACL is not aware of any actual harm being suffered as a result of the Medlab Cyberattack.

104. While there is no evidence that any individuals suffered any loss or damage because of ACL's contraventions of s 13G(a) of the Privacy Act that occurred by reason of ACL's breaches of ss 26WH and 26WK of the Privacy Act, those breaches did mean there was a delay in the Commissioner being notified of an eligible data breach which accordingly delayed the Commissioner's ability to perform her statutory functions, including monitoring notification of individuals which will allow those individuals to protect themselves from the risk of harm, loss and damage associated with that eligible data breach.

105. Additionally, the failure to conduct the reasonable and expeditious assessment resulted in an incorrect conclusion by ACL by 21 March 2022 that there were not reasonable grounds to believe that an eligible data breach had occurred in relation to Medlab.

Whether ACL has previously been found by a court to have engaged in similar conduct

106. ACL has not previously been found by a court to have contravened provisions of the Privacy Act or otherwise engaged in similar conduct.

Whether ACL obtained a financial gain or benefit from the contraventions

107. ACL did not obtain any direct financial gain or benefit from the contraventions.

Whether contraventions arose from the conduct of senior management

108. ACL's senior management were involved in:

a. the decision-making around the integration of Medlab's IT systems into ACL's core IT environment; and

b. ACL's response to the Cyberattack, including in determining whether and when the Cyberattack amounted to an eligible data breach,

as described in this SAFA.

109. There is no evidence, and it is not alleged, that any of the contraventions of s 13G(a) of the Privacy Act arose from deliberate misconduct by any of ACL's senior management.

Whether ACL had a corporate culture of compliance and remediation

110. Despite the contraventions of s 13G(a) of the Privacy Act, throughout the Relevant Period, ACL sought to and did improve its corporate culture of compliance with respect to its cybersecurity capabilities.

111. Prior to the Relevant Period, in 2021, ACL engaged StickmanCyber to conduct a review of its cybersecurity framework to determine ACL's cybersecurity capabilities at that point in time which ACL could then use as a reference point to identify the aspects of its cybersecurity capabilities which should be changed or improved. On 26 May 2021, StickmanCyber prepared a report which benchmarked ACL against the National Institute of Standards and Technology Cybersecurity Framework (**NIST**) (**2021 report**). It identified various deficiencies and areas for improvement in ACL's cybersecurity processes and controls. The 2021 report gave ACL an overall risk assessment rating of [redacted] out of 4 on the NIST Framework. This placed ACL between [redacted]

112. Following its receipt of the 2021 report, ACL developed a program of works to uplift the company's cybersecurity capabilities (**Cybersecurity Uplift Program**). The Cybersecurity Uplift Program was approved by the Board of ACL on 1 July 2021.

113. Following its implementation of the Cybersecurity Uplift Program, ACL conducted a further review of ACL's cybersecurity processes and controls against NIST in 2022, in which StickmanCyber prepared a report dated 29 September 2022 (**2022 report**). The 2022 report gave ACL an overall risk assessment rating of [redacted] out of 4 on the NIST Framework, which placed ACL between [redacted]

114. In October 2022, ACL engaged McGrath Nicol to further review ACL's cybersecurity capabilities. That review concluded that ACL was at the early stages of its cyber security journey, where it was working with StickmanCyber to address defined remediation initiatives. McGrath Nicol's workshop and review of documentation found that there were good areas of security in place with opportunities to improve further. It was found that there were ongoing effort and initiatives on the part of ACL to address weak security control areas, and good governance driving the improvement plans through quarterly security committees.

115. As part of the Cybersecurity Uplift Program, ACL implemented, among others, the following enhancements to its cybersecurity capabilities:

a. [redacted];

b. [redacted];

c. since late August 2022, ACL has required all its employees to undertake regular cybersecurity awareness training provided through a specialist third party vendor. [redacted];

i. [redacted];

ii. [redacted]; and

iii. [redacted].

[redacted] of ACL's employees have undertaken that training;

d. in August 2023, ACL appointed an experienced and credentialed full-time Chief Information Security Officer with responsibility for information security across the organisation;

e. [redacted];

f. [redacted].

116. The above improvements in ACL's cybersecurity capabilities lessens the likelihood that ACL will engage in future contraventions of s 13G of the Privacy Act, including by reason of a breach of APP 11.1 and ss 26WH(2) and 26WK(2) of the Privacy Act.

Size and financial position of ACL

117. As stated at [7] above, ACL is and was during the Relevant Period one of the largest private hospital pathology businesses in Australia, generating revenue of $674.4 million in the financial year ending June 2021, $995.6 million in the financial year ending June 2022 and $697.1 million in the financial year ending June 2023. As at 30 June 2022, ACL employed approximately 5,400 staff. As at 30 June 2023, ACL employed approximately 5,115 staff.

118. ACL's net operating income, profit before income tax and net profit for each year before, of and after the Relevant Period was as follows:

Year	Net Operating Income (Annual Turnover)	Profit Before Income Tax	Net Profit
2021	$674.4M	$140M	$88.7M
2022	$995.6M	$266.6M	$178.2M
2023	$697.1M	$70.3m	$41.7M

Co-operation with the Office of the Australian Information Commissioner

119. In or around December 2022, the Office of the Australian Information Commissioner (**OAIC**) commenced an investigation into the acts and practices of ACL and Medlab in relation to the Medlab Cyberattack. ACL cooperated with the OAIC in its investigation, producing multiple written responses and approximately 12,000 documents.

120. Following the commencement of these proceedings, and before the hearing on liability, ACL has admitted the contraventions the subject of the proceeding by way of filing this SAFA.

Contrition

121. ACL's Chief Executive Officer has apologised that the Medlab Cyberattack occurred in the terms set out in the 27 October 2022 ASX announcement extracted at [58] above.

Dated: 29 August 2025

DLA Piper

Signed by DLA Piper Australia
Lawyer for the Applicant

Gilbert + Tobin

Signed by Gilbert & Tobin
Lawyer for the Respondent