NOTICE OF FILING

Details of Filing

Document Lodged:	Concise Statement
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	24/11/2023 9:11:00 AM AEDT
Date Accepted for Filing:	24/11/2023 9:13:41 AM AEDT
File Number:	NSD1287/2023
File Title:	AUSTRALIAN INFORMATION COMMISSIONER v AUSTRALIAN CLINICAL LABS LIMITED ACN 645 711 128
Registry:	NEW SOUTH WALES REGISTRY - FEDERAL COURT OF AUSTRALIA

SEAL OF THE FEDERAL COURT OF AUSTRALIA

Sia Lagos

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date of the filing of the document is determined pursuant to the Court's Rules.

Concise Statement

No. of

Federal Court of Australia

District Registry: New South Wales

Division: General

Commercial and Corporations Practice Area (Regulator and Consumer Protection)

AUSTRALIAN INFORMATION COMMISSIONER

Applicant

AUSTRALIAN CLINICAL LABS LIMITED (ACN 645 711 128)

Respondent

A INTRODUCTION

1 The Australian Information Commissioner (**AIC**) alleges that, during the period 26 May 2021 to 29 September 2022 (**Relevant Period**), the Respondent (**ACL**) seriously interfered with the privacy of approximately 21.5 million individuals, whose personal information it held, in contravention of s 13G of the *Privacy Act 1988* (Cth) (**Act**), by failing to take reasonable steps to protect that personal information from unauthorised access or disclosure, in breach of Australian Privacy Principle (**APP**) 11.1(b). These failures left ACL vulnerable to cyberattack.

2 The AIC also alleges that, when a cyberattack on ACL did occur, in around February 2022, which exposed the personal information of at least 223,269 individuals, ACL failed to carry out a reasonable assessment of whether it amounted to an eligible data breach and then failed to notify the AIC as soon as practicable, in contravention of ss 26WH(2) and 26WK(2) of the Act. These were further serious interferences with the privacy of individuals in contravention of s 13G of the Act.

B IMPORTANT FACTS GIVING RISE TO THE CLAIM

3 ACL was incorporated on 6 November 2020. It replaced its predecessor company, Clinical Laboratories Pty Ltd (**Clinical Labs**) as the ultimate holding company of the ACL group of companies on 16 December 2020. ACL is a public company listed on the Australian Securities Exchange. It is one of the largest private hospital pathology businesses in Australia.

4 ACL's business centrally involves collecting and holding individual patients' health information. ACL collects other personal information from patients in order to provide test results and issue invoices, such as personal identifying and contact information, Medicare card copies and numbers, and passport numbers.

5 ACL generated revenue of $647 million in the financial year ending in June 2021 and $995.6 million in the financial year ending in June 2022. As at 30 June 2022, ACL employed approximately 5,400 staff.

6 During the Relevant Period ACL was, and remains, an APP entity within the meaning of s 6 of the Act and was, and is, required to comply with the APPs in its handling of personal information.

Filed on behalf of (name & role of party) Australian Information Commissioner, Applicant
Prepared by (name of person/lawyer) John Fogarty
Law firm (if applicable) DLA Piper Australia
Tel 0401 063 700 Fax
Email john.fogarty@dlapiper.com
Address for service (include state and postcode) Level 15, 80 Collins Street, Melbourne, VIC 3000

7 In late 2021, ACL acquired the assets of Medlab Pathology (**Medlab**), including Medlab's computer and communications hardware, computer and information technology systems and equipment and software. Medlab was a privately owned pathology business providing services in New South Wales and Queensland, including prenatal genetic testing, fertility assessments and testing for sexually transmitted diseases. Medlab processed approximately 1.5 million pathology patient episodes per annum and held sensitive personal information relating to more than 100,000 individuals. In addition to collecting and holding individual patients' health and contact information, Medlab collected and held customer credit card and payment details.

8 Before acquiring Medlab, ACL did not undertake a sufficient cybersecurity assessment in respect of the risks associated with the Medlab computer network, the personal information held by Medlab, or the steps it could take to address any cybersecurity risks associated with its acquisition of that network. In particular, ACL was aware prior to the acquisition that Medlab had not conducted any IT pentetration test, vulnerability assessment or IT security audit in the preceding three years. From late 2021, ACL owned and controlled Medlab's computer network, which it operated separately from ACL's computer network. Further, from that time, the IT team responsible for the day-to-day operations of the Medlab computer network reported to ACL's Chief Information Officer (**CIO**). ACL planned to transfer Medlab's network to ACL's network and decommission the Medlab servers. This did not occur until around July 2022.

ACL's cybersecurity framework

9 In the Relevant Period, ACL was required to encrypt payment card information it held at rest in accordance with the Payment Card Industry Data Security Standard (**PCIDSS**). ACL was required by APP 1.2(a) to implement practices, procedures and systems relating to its functions or activities that ensured it complied with the APPs. In particular, APP 11.1(b) required ACL to take such steps as were reasonable in the circumstances, to protect the personal information it held from misuse, interference and loss, and from unauthorised access, modification or disclosure. The content of the obligation which APP 11.1(b) imposes will vary according to the nature and circumstances of an APP entity, the amount and sensitivity of the personal information it holds, the possible adverse consequences for an individual in the case of a breach, the practical implications of implementing the security measure, whether a security measure is in itself privacy invasive, applicable laws and industry standards from time to time.

10 During the Relevant Period, ACL's cybersecurity framework comprised the policies, controls and resources identified in **Annexure A**.

11 ACL could have adopted various cybersecurity standards and frameworks as benchmarks, to improve its cybersecurity capabilities, and to ensure compliance with APP 11.1(b). Relevantly, during the Relevant Period:

(a) ACL selected the National Institute of Standards and Technology Cybersecurity Framework (**NIST**) for the purposes of such benchmarking;

(b) ACL conducted audits of its cybersecurity framework against the International Organization for Standardization's Information Security Management Standards (**ISO27001**) and stated in its annual report that it had an information security policy and standards framework established in accordance with ISO27001;

(c) ACL's insurance broker, Aon Risk Services Australia Limited identified "Non-negotiable Cyber Security Controls" which Aon described as the insurers' minimum cybersecurity baseline for all businesses, regardless of industry or size (**ACL Insurer's requirements**); and

(d) the Australian Cyber Security Centre (**ACSC**) had identified eight key controls that it considered "essential" to preventing cyberattacks (**E8**).

12 Having regard to its size, resources, the nature and volume of the sensitive personal information it held, and the possible adverse consequences for an individual in the case of a breach, during the Relevant Period it was reasonable for ACL to adopt some combination sufficient to its circumstances, or alternatively, all, of the following measures to protect the personal information it held:

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

(f) [redacted]

(g) [redacted]

(h) [redacted]

(i) [redacted]

None of these measures was implemented by ACL during the Relevant Period.

13 From at least the commencement of the Relevant Period (26 May 2021), ACL was aware of serious deficiencies in its cybersecurity framework. In particular:

(a) in March 2019, Clinical Labs' (now ACL's) CIO provided a report to the Clinical Labs Board setting out a plan to "commence review and planning for an IT security framework" later that year;

(b) ACL's predecessor had conducted a review in 2020, in the form of an *Information Security Management System Maturity Assessment Report* from a cybersecurity firm, Content Security in May 2020 (**ISO audit**). [redacted]

(c) ACL conducted a review in 2021, in which a cybersecurity firm engaged by Clinical Labs, StickmanCyber, prepared a report dated 26 May 2021 (**2021 Report**). ACL provided a copy of the ISO audit to StickmanCyber for the preparation of the 2021 Report. The 2021 Report benchmarked ACL against NIST. [redacted]

(d) 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**). [redacted]

The Cyberattack

14 On or before 25 February 2022, a malicious actor known as the Quantum group attacked the Medlab computer network operated by ACL (the **Cyberattack**). ACL does not know the time or method of the Cyberattack. In the Cyberattack, the Quantum group exfiltrated 86 gigabytes of data, including identifying information such as passport numbers, health information, and financial information such

as credit card details with names, card numbers, expiry and ccv of at least 223,269 individuals. That information was personal information and sensitive information, as defined in s 6 of the Act.

15 On or before 16 June 2022, the exfiltrated information was published on the dark web.

16 An employee first became aware of the Cyberattack at around 5.00 am 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 which stated: “During the period your network was under our control, we downloaded a huge volume of information… The 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 all your information will be posted on our site.”

17 About fifteen minutes later, the employee notified the Medlab IT team of the ransom demand. By 9.00am on 25 February 2022, the ransom note had appeared on other computers on the Medlab network in Brisbane and Sydney and files on those computers were encrypted to “.quantum”.

Response to the Cyberattack

18 ACL did not have a dedicated cybersecurity team. Its response to the Cyberattack was led by an IT Team Leader and was overseen by ACL’s CIO and Head of Technical Services. None of those personnel had formal cybersecurity qualifications or experience in responding to a cyberattack.

19 At around 12.45pm on 25 February 2022, ACL’s Head of Technical Services provided the IT Team Leader with ACL’s *Ransomware and Malware Outbreak (Windows)* playbooks. Before then, the IT Team Leader had not seen, used, or received training on these playbooks. She had received no cybersecurity training at all. The playbooks were general in nature and recommended steps for technologies not used on the Medlab network. Critical steps specified in the playbooks were not implemented in the incident response. For example, ACL did not analyse the ransomware to determine its capabilities or take system images of infected systems before wiping them.

20 On 25 February 2022, at or around 1.32pm, ACL instructed StickmanCyber to assist its response to the Cyberattack. The scope of that engagement was not defined and it was unclear who was to lead the response. StickmanCyber remained involved in ACL’s incident response until 1 March 2022, spending 44.5 hours on the engagement. In this time, StickmanCyber:

(a) deployed monitoring agents on only three of at least 121 computers subject to ransomware;

(b) suggested that ACL prepare a statement that there had been a malware incident. ACL did not act on this suggestion;

(c) reviewed the available one hour of backed-up firewall logs, conducted dark web scans and concluded that no data had been exfiltrated;

(d) concluded, based only on the limited work conducted since its engagement, that the attack vector was through a phishing email addressed to the employee who had alerted ACL to the ransomware attack; and

(e) did not investigate the possibility that the threat actor may have established persistence mechanisms to retain access to the Medlab network.

21 Having received the ransom note from the Quantum group and StickmanCyber’s advice on the Cyberattack, by at least 1 March 2022, ACL was aware that the Quantum group had gained unauthorised access to the Medlab computer network and encrypted files containing personal information, including sensitive health information.

Notification of eligible data breach to the AIC

22 On 14 March 2022, ACL’s Head of Technical Services asked StickmanCyber whether it was necessary to obtain legal advice about whether the Cyberattack amounted to an eligible data breach under the

Act. In response, StickmanCyber stated "…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."

23 On 21 March 2022, ACL's CIO and General Counsel separately asked the IT Team Leader who conducted the incident response to confirm whether the Cyberattack had resulted in exfiltration of data. Initially the IT Team leader responded to the CIO stating that: "As per firewall logs and Stickman's findings we did not see any high data transmission on the firewall and also our main SERVERs with DATABASE were not affected. There has been no call for ransom demand as far as IT is aware."

24 Later, after speaking with the General Counsel, the IT Team Leader sent a further email stating: "As per information available to IT Department there was no unauthorized access, disclosure, or loss of any personal information, health information, or company sensitive data as a result of the incident which began on the 25th Feb 2022 to date."

25 Based on the communications in [22] to [24], on 21 March 2022, ACL determined that the Cyberattack was not an eligible data breach. It did so, in circumstances in which it was aware that:

(a) a threat actor had gained unauthorised access to the Medlab network where it held personal information and sensitive health information;

(b) at the time of the Cyberattack, Medlab's firewall logs were only retained for an hour before being deleted, such that, when ACL started checking Medlab's firewall logs around 9am on the day of the Cyberattack, it was limited to those one hour prior and was not able to trace any earlier activities by the threat actor on the firewall; and

(c) that dark web monitoring had ceased after less than five days, ACL had no inhouse forensic or incident response capability, and the IT Team Leader had no cybersecurity training and credentials.

26 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 reminding ACL that it may be required to notify the AIC and affected individuals (**first ACSC notification**). ACL did not reopen its investigation or revisit its assessment that the Cyberattack was not an eligible data breach. It did not undertake further dark web scanning or seek further information from the ACSC. It instead provided the ACSC with details of the incident and informed the ACSC that no data had been exfiltrated.

27 On 16 June 2022, at 10.26am, the ACSC sent ACL a second notification (**second ACSC notification**), which stated: "The [ACSC] has received a report from a trusted third party regarding a potential data breach impacting [Medlab]. Through monitoring of darkweb sources, it has come to 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…"

28 By 2.53pm on 16 June 2022, ACL was satisfied that data had been exfiltrated from its systems containing complete credit card information and personal health information and the data was publicly accessible. However, ACL did not give the AIC a statement in the form required under s 26WK of the Act until 10 July 2022. In the 24-day intervening period, ACL did not receive any new information about the breach.

C ALLEGED CONTRAVENTIONS OF THE ACT

Breach of APP 11.1(b)

29 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, *inter alia*, from unauthorised access or disclosure.

30 During the Relevant Period, having regard to its size, resources and the nature and volume of the sensitive personal information it held, and the possible adverse consequences for an individual in the case of a breach, ACL did not take such steps as were reasonable in the circumstances to protect the information it held from unauthorised access or disclosure. ACL thereby breached APP 11.1(b) and

interfered with the privacy of the approximately 21.5 million individuals whose personal information it held. There were deficiencies in the form and implementation of the cybersecurity framework identified in **Annexure A**.

31 Further, or alternatively to [30], during the Relevant Period, and having regard to its size, resources and the nature and volume of the sensitive personal information it held, APP 11.1(b) required ACL to take some combination sufficient to its circumstances, or alternatively, all, of the steps alleged at [9], and [12(a) – 12(i)] to protect the personal information it held from unauthorised access.

32 ACL failed to take these steps during the Relevant Period. In particular:

(a) the firewall logs on the Medlab network deleted after one hour and there was no monitoring of security alerts, as a result of which ACL was unable to determine when the Cyberattack occurred and whether it had resulted in the exfiltration of data;

(b) [redacted]

(c) ACL did not undertake sufficient assessment in respect of the risks associated with the Medlab computer network, the personal information held by Medlab, or the steps it could take to address any cybersecurity risks associated with ACL's acquisition of that network;

(d) [redacted]

(e) [redacted]

(f) [redacted]

(g) [redacted]

(h) [redacted]

(i) [redacted]

(j) [redacted]

(k) [redacted]

33 By reason of the matters alleged at [30] to [32], during the Relevant Period, ACL breached APP 11.1(b) and therefore interfered with the privacy of the approximately 21.5 million individuals whose personal information it held.

34 The failures alleged at [30] to [33] were serious and systemic, in that deficient systems and processes were the root of ACL's failure to take reasonable steps. For example, ACL's IT budget for 2022 was $1.3 million and its cybersecurity budget was $350,000, which was significantly lower than that of

industry standards, for a company of ACL's size and having regard to the volume and nature of the personal information it held throughout the Relevant Period.

Contravention of s 26WH of the Act

35 Under s 26WH of the Act, upon becoming aware that there were reasonable grounds to suspect that there may have been an eligible data breach (as defined in s 26WE(2)(a)), but before it became aware of reasonable grounds to believe that there was an eligible data breach, ACL was required to carry out a reasonable and expeditious assessment of whether there were reasonable grounds to believe that the relevant circumstances amounted to an eligible data breach and to take all reasonable steps to ensure that the assessment was completed within 30 days.

36 In the circumstances alleged in [14] to [20], by 1 March 2022, ACL had reasonable grounds to suspect that there may have been an eligible data breach. In particular, by that date, ACL was aware that:

(a) at some time prior to 25 February 2022, a threat actor had gained unauthorised access to the Medlab network where ACL held personal information of its customers, including sensitive health information;

(b) files on the Medlab network had been encrypted with the .quantum extension and ACL had received a ransom note from the Quantum group stating that it had accessed ACL's systems, "downloaded a huge volume of information" and would disclose the information if a ransom was not paid;

(c) StickmanCyber had conducted a limited investigation into the Cyberattack by deploying monitoring agents on only 3 of at least the 121 computers subject to the ransomware deployed by the threat actor, and the scope of its engagement did not require it to conduct an investigation into the threat actor and its attack traits, to determine whether data was likely to have been exfiltrated;

(d) ACL's, and StickmanCyber's, assessment of the Cyberattack was based on a review of only one hour of firewall logs, which it did not access until approximately four hours after the ransom note was first downloaded;

(e) the ACL personnel who were responsible for carrying out the assessment were not appropriately qualified or experienced and had received no or minimal cybersecurity training;

(f) ACL's procedures for responding to a ransomware attack were inadequate (having regard to the conclusions in the earlier 2021 Report).

37 The matters alleged at [36] supplied reasonable grounds to suspect that:

(a) there had been unauthorised access to the personal information of individual customers and patients that ACL held by reason of its control over the Medlab IT systems at that time; and

(b) the access would be likely to result in serious harm to any of the individuals to whom the information related.

38 In circumstances where ACL failed to carry out any assessment, or a reasonable assessment, of whether there were reasonable grounds to believe that the Cyberattack amounted to an eligible data breach and where it did not take all reasonable steps to ensure that the assessment was completed within 30 days, ACL contravened s 26WH(2) of the Act.

Contravention of s 26WK of the Act

39 Under s 26WK of the Act, upon becoming aware that there were reasonable grounds to believe that there had been an eligible data breach, ACL was required as soon as practicable to prepare a statement in accordance with s 26WK(3) and give a copy of that statement to the AIC.

40 By reason of the matters of which ACL was aware as at 1 March 2022, as alleged at [38], together with its awareness of the first ACSC notification on 25 March 2022, by 25 March 2022, ACL was aware of matters that constituted reasonable grounds to believe that the Cyberattack was an eligible data

breach. It was practicable for ACL to notify the AIC of the Cyberattack within a matter of 2 – 3 working days of 25 March 2022.

41 Alternatively, by reason of the matters of which ACL was aware as at 1 March 2022, as alleged at [36], together with its awareness of the first ACSC notification on 25 March 2022, and the second ACSC notification on 16 June 2022, by 16 June 2022, ACL was aware of matters that constituted reasonable grounds to believe that the Cyberattack was an eligible data breach. It was practicable for ACL to notify the Commissioner of the Cyberattack within 2 – 3 working days of 16 June 2022.

42 ACL did not notify the AIC of the Cyberattack in accordance with s 26WK(3) of the Act until 10 July 2022. Accordingly, by reason of the matters alleged in [40], or alternatively, [41], ACL contravened s 26WK of the Act.

Contravention of 13G of the Act

43 Under s 13(1) of the Act, an act or practice of an APP entity is an interference with the privacy of an individual if it breaches an APP in relation to the personal information about the individual. Under s 13(4A), contraventions of ss 26WH(2) or 26WK(2) are taken to be acts that interfere with the privacy of an individual.

44 Under s 13G(a) of the Act, an entity will be liable for a civil penalty if it does an act, or engages in a practice, that is a serious interference with the privacy of an individual. With respect to the allegations of contravention of APP 11.1(b), the AIC contends that a contravention of s 13G(a) arises in respect of each of the approximately 21.5 million individuals whose personal information ACL held throughout the Relevant Period. With respect to the contraventions of ss 26WH(2) and 26WK(2) of the Act, as each contravention is taken to be an interference with the privacy of an individual under s 13(4A) of the Act, the AIC contends that that ACL engaged in two further contraventions of s 13G(a) of the Act.

45 Each contravention within the Relevant Period attracted a maximum penalty of $2,220,000 by reason of s 13G of the Act in force during the Relevant Period, and s 82(5)(a) of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)).

46 Each of ACL's breaches of APP 11, and its contraventions of ss 26WH(2) and 26WK(2) of the Act, were serious including because they affected a large number of individuals and concerned sensitive personal information.

D RELIEF SOUGHT

47 The AIC seeks the relief set out in the accompanying Originating Application, including declaratory relief under s 21 of the *Federal Court of Australia Act 1976* (Cth), orders for civil pecuniary penalties under s 80U of the Act, and costs.

E ALLEGED HARM

48 A fundamental principle underpinning the Act is that APP entities are responsible for the personal information they hold. ACL did not have regard to this principle throughout the Relevant Period, in that it failed to adequately manage cybersecurity risk congruent with the nature and volume of sensitive information it held, its size, and the risk profile of its sector. ACL had not invested sufficiently in the specialist cybersecurity staff or the policies, practices and controls reasonably required to protect the information it held.

49 Another fundamental principle underpinning the Act is that, when a data breach does occur, organisations are responsible for taking steps to notify the AIC so as to manage and minimise the risks associated with a data breach. Contrary to this principle, after ACL was the subject of the Cyberattack, ACL delayed notifying the AIC.

50 ACL's failure to take reasonable steps commensurate with protecting the highly sensitive information it held exposed that information to the risk of misuse. That risk materialised when ACL was the subject of a cyberattack and a malicious actor accessed personal identifying information, health information and credit card details and posted this information on the dark web, exposing approximately 223,269

individuals to potential emotional distress and the material risk of identity theft, extortion and financial crime.

This concise statement was prepared by John Fogarty and Wei Xin Lee of DLA Piper Australia, and settled by Ruth Higgins SC and Emma Bathurst of Counsel.

Annexure A – ACL's cybersecurity framework in the Relevant Period

Resources

1 ACL's FY22 dedicated cyber budget was $350,000. ACL's FY22 IT budget was $1.3 million.

2 ACL did not have full-time personnel dedicated to cybersecurity. ACL's Head of Technical Services was also responsible for IT Security.

3 The team responsible for managing the IT systems within ACL's Medlab environment comprised of 5 people.

Policy framework

4 ACL had the following cybersecurity or cybersecurity-related policies and standards:

(a) Information Technology Manual – Data Security – dated 27 May 2019;

(b) Computer Security, Policies & Procedure Manual – dated 10 January 2020 and specific to Medlab;

(c) Malware and Vulnerability/Patch Management Standard Policy – dated 20 May 2020 and revised on 1 September 2022, at which point the document was renamed Malware and Vulnerability/Patch Management Standard;

(d) Identity and Access Management Standard Policy – dated 20 May 2020 and revised on 1 September 2022;

(e) Cyber Security Policy – dated 20 May 2020 and revised on 1 September 2022;

(f) Security Incident Management Standard – dated 20 May 2020 and revised 1 September 2022;

(g) Mobile Device and Remote Access Standard – dated 20 May 2020 and revised on 2 September 2022;

(h) Secure Deletion and Disposal Standard Policy – dated 12 August 2020 and revised 1 September 2022, at which point the document was renamed Secure Deletion and Disposal Standard;

(i) IT Acceptable Use Policy – dated 10 December 2020 and revised on 1 September 2022;

(j) External Supplier IT Security Standard – dated 10 February 2021 and revised 1 September 2022;

(k) Information Technology Disaster Recovery Plan – dated 14 January 2021;

(l) Data breach playbook – dated August 2021;

(m) Internal compromise playbook – dated August 2021;

(n) Malware outbreak playbook – dated August 2021;

(o) Ransomware playbook – dated August 2021;

(p) Information Security Incident Management Plan (draft) – dated 9 September 2021;

(q) Asset Management Standard – dated 13 October 2021 and revised on 1 September 2022;

(r) Information Security Policy – dated 1 September 2022; and

(s) IT Software Currency N-2 Policy – dated 1 September 2022.

5 In addition, ACL had the following policy and standard documents which were not specific to cybersecurity risks:

(a) Change Management Standard – dated 20 May 2020, revised 26 June 2020 and 1 September 2022;

(b) Incident Management Policy – dated 15 October 2020 which mainly related to patient care;

(c) Risk Management Standard – dated 6 October 2021; and

(d) Incident Management Procedure – dated 27 September 2022.

Process and controls

6 ACL had the following cybersecurity controls in place:

(a) ACL policy was for two factor authentication to apply to access to confidential information, to remotely access the network or to have administrator access, however MFA was not comprehensively implemented for the ACL network and was not required at all for remote access into the Medlab network;

(b) Domain Administration privilege access was restricted to 42 user accounts;

(c) [redacted]

(d) [redacted]

(e) ACL was using basic malware detection for emails received on the Medlab network. ACL used the Exchange Online Protection email security control within Office 365 for this purpose;

(f) The Medlab network had a limited amount of security monitoring and incident notification capability; and

(g) Firewall logs on the Medlab network were retained for one hour before being deleted.

Certificate of lawyer

I John Fogarty certify to the Court that, in relation to the statement of claim filed on behalf of the Applicant, the factual and legal material available to me at present provides a proper basis for each allegation in the pleading.

Date: 2 November 2023

Signed by John Fogarty

Lawyer for the Applicant