

Thursday, 27 October 2022

Cyber Security Incident and notifiable data breach – Medlab Pathology

Australian Clinical Labs Limited (ASX: ACL) (**ACL** or **Company**) advises that Medlab Pathology, a pathology business acquired by ACL in December 2021 (**Medlab**), has experienced a notifiable cyber incident involving personal information of some of Medlab's patients and staff.

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.

The Office of the Australian Information Commissioner (**OAIC**) has been notified and both the OAIC and the Australian Cyber Security Centre (**ACSC**) have been kept abreast of the progress of the forensic investigations into the incident.

To date, there is no evidence of misuse of any of the information or any demand made of Medlab or ACL.

The compromised Medlab server has been de-commissioned and is no longer in use. ACL's broader systems and databases are not affected by the incident.

Medlab became aware of an unauthorised third-party access to its IT system in February 2022. ACL immediately coordinated a forensic investigation led by independent external cyber experts into the Medlab incident. At the time, the external forensic specialists did not find any evidence that information had been compromised.

In March, the company was contacted by the ACSC outlining that it had received intelligence that Medlab may have been the victim of a ransomware incident. The company responded to the request for information and confirmed that to its knowledge the company did not believe that any data had been compromised.

In June, ACL was again approached by the ACSC, which informed ACL that it believed that Medlab information had been posted on the dark web. ACL took immediate steps to find and download this highly complex and unstructured data-set from the dark web and made efforts to permanently remove it.

Following advice from privacy and legal specialists in cyber matters, ACL implemented a program to determine the nature of the information involved and any individuals that could be at risk of serious harm as a result of the incident.

Given the highly complex and unstructured nature of the data-set being investigated, it has taken the forensic analysts and experts until now to determine the individuals and the nature of their information involved.

ACL's view is that, given the nature of its relationship with the affected individuals, the most effective way to minimise the potential harm to those individuals and the wider body of Medlab's patients, is to directly contact the individuals at risk by way of individually tailored notifications as soon as practicable.

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."*

Further information on the incident is available at <https://medlab.com.au/>.

– ENDS –

This announcement was authorised for release to ASX by the Board of ACL.

For further information regarding this announcement, please contact:

Investors

Eleanor Padman
Company Secretary
Email: investors@clinicallabs.com.au
Phone: +61 (0) 422 002 918

Media

Clive Mathieson, Sue Cato
Email: clive@catoandclive.com
cato@catoandclive.com
Phone: +61 (0) 411 888 425
+61 (0) 419 282 319

About Australian Clinical Labs

ACL is a leading Australian private provider of pathology services. Our NATA accredited laboratories perform a diverse range of pathology tests each year for a range of clients including doctors, specialists, patients, hospitals and corporate clients. ACL is one of the largest private hospital pathology businesses nationally. ACL is focused on its mission of combining talented people, and medical and scientific leadership, with innovative thinking and technologies to empower decision making that saves and improves patients' lives.