FOR INTERNAL USE ONLY

ASIC
Australian Securities & Investments Commission

Response to recent cyber incidents		
November 2022		
Contact	**Senior Executive Leader**	**Executive Director**
s 22 [redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Key Messages

- With all of the cyber incidents the first priority is addressing consumer harms. We continue to work closely with the ACCC and APRA, the government and a range of other agencies through a number of forums. We work closely with the ASX in relation to real-time disclosure issues associated with cyber incidents.
- The extent of potential harm to millions of Australians arising from the theft of sensitive and identity information requires a whole of government approach to minimise harm to consumers, and ASIC is participating in this response as appropriate.
- ASIC has long taken a strong interest in the cyber resilience of Australian financial services and markets.
- The RI Advice case is one of the first cases ever run in Australia on what's expected of financial services licensees in this area of cyber security and cyber resilience. This decision confirms that AFS licensees must have adequate technological systems, policies and procedures to ensure sensitive consumer information is protected.
- ASIC expects directors to ensure their organisation's risk management framework adequately addresses cybersecurity risk, and that controls are implemented to protect key assets and enhance cyber resilience. Directors should also consider whether they are required to make public disclosure.
- In March 2022 ASIC made revision to the Market Integrity Rules to enhance technological and operational resilience obligations on market operators and participants. These take effect in March 2023 and cover matters such as cyber incidents and information security in addition to other matters.
- The recent cyber incidents and subsequent data theft at Optus, Medibank / AHM, Australian Clinical Labs and My Deal are a wake-up call and this type of attack could happen to any range of entities in the country.

Optus - Consumer Protection response

- ASIC contributed comments on the data sharing provisions in the telecommunications regulation as they relate to financial services firms. This allowed firms to implement targeted fraud protection mechanisms. Data sharing under the telecommunication regulations has been limited to APRA regulated entities and firm that support them. ASIC regulated entities may be considered at a later stage.
- ASIC is having regular engagement with industry associations and Big 4 banks to monitor risk of fraud/scams and outline expectations of heightening monitoring and controls.
- ASIC directly engaged with Market Intermediaries to communicate expectations that they exercise extra vigilance in verifying and managing customers' personal information.

- Sarah Court & s 22 attended a Scams Roundtable meeting called by the Assistant Treasurer with a focus on consumer messaging re the Optus breach and general ideas for the Anti-Scams centre.

Optus - Enforcement aspects

- ASIC continues to engage closely with ACMA, OAIC and other relevant agencies on the regulatory response to the Optus data breach.

- Optus does not hold an Australian Financial Services License and ASIC is not the lead regulator in cases like this This means that ASIC's role in investigating and enforcing the law is likely to be limited to any failure by the directors or senior officers of Optus to discharge their duties to the company.

- If there is information that may suggest the directors or officers of Optus have contravened the Corporations Act, ASIC will work with the OAIC, ACMA and other relevant agencies to determine how those suspected contraventions might best be, and most efficiently, investigated.

Medibank - ASIC's regulatory remit

- APRA is the principle financial regulator of Medibank including in relation to cyber risk management obligations. Medibank is subject to mandatory information security standards under APRA prudential standards.
- Medibank is an ASX listed entity and has disclosure and other obligations in this capacity.
- They are an Authorised Representative of four Australian Financial Services licensees. This is in relation to the distribution of other insurance products (ie life insurance, funeral insurance, travel insurance and pet insurance).
- ASIC has made enquiries of the four licensees that we regulate regarding the impact (if any) of the Medibank data breach on these other (non-health) insurance products.
- Consumer protection remains the immediate priority for ASIC activities.

Australian Clinical Labs (ACL)

- ACL is an ASX listed entity, who's wholly owned subsidiary MedLabs experienced a cyber incident in February 2022. Following an initial approach from the ACSC in March about a likely cyber attack, they were again contacted in July, advising that it appeared client information was available on the dark web.
- On 27 October an announcement was made to the market, four months after ACL was advised of the release of the data on the dark web. ASIC is making relevant enquiries around the timing of this disclosure.