Article Information

Authors: Craig Subocz, Jan David Hohmann
Service: Corporate & Commercial, Cyber Security, Intellectual Property & Technology
Sector: Financial Services

Federal Court highlights adequate cybersecurity measures as a legal obligation for financial services licence holders

The Federal Court shone a spotlight on cybersecurity measures for Australian financial services (AFS) licence holders, and Australian companies generally, when it held that financial planner RI Advice breached the law by failing to implement adequate cybersecurity protection measures to protect client confidential information. In the wake of the decision, companies need to identify gaps in their cybersecurity risk management and fix them fast.

The Federal Court held that cybersecurity measures implemented by RI Advice Group Pty Ltd (**RI Advice**) were inadequate after nine cybersecurity incidents between June 2014 and May 2020 affected the systems of its authorised representatives (**ARs**). The Federal Court proceedings were brought by the Australian Securities and Investments Commission (**ASIC**) against RI Advice. As a result of these incidents, RI Advice clients received phishing emails, ARs' computer systems were accessed without authorisation and attacked by ransomware, and client information was exposed. RI Advice implemented measures to reduce the risk of cybersecurity incidents from May 2018 onwards, but accepted that, prior to May 2018, it did not have adequate documentation, controls and a risk management system. RI Advice engaged a security consultant in May 2018 to develop a program to increase cyber resilience. A "Cyber Resilience Initiative" program was launched internally in 2019, but not to its ARs until January 2020. The rollout of the program was not completed until August 2021. RI Advice accepted that it took too long to implement, and to ensure that, cybersecurity measures were implemented by its ARs, and accepted that it should have had a more robust implementation of its program.

RI Advice accepted that, pursuant to sections 912A(1)(a) and (h) of the *Corporations Act 2001* (Cth), as part of its statutory duty to do all things necessary to ensure that it provided financial services efficiently, honestly and fairly, it must identify risks that could affect the provision of financial services (including in relation to cybersecurity and cyber resilience) and to have adequate documentation, controls and risk management systems to manage cybersecurity risk and cyber resilience across its ARs.

The Court considered cybersecurity to involve the ability of an organisation to protect and defend the use of cyberspace from attacks, and cyber resilience to involve the ability of a company to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber sources.

The Court noted that cybersecurity risks evolve over time, and it is not possible to reduce cybersecurity risks to zero, but it is possible to materially reduce the risk to an acceptable level through adequate documentation and controls. RI Advice accepted that it did not have adequate controls and risk management systems in respect of cybersecurity risks prior to May 2018. The Court held that, between May 2018 and August 2021, the delay in implementing the "Cyber Resilience Initiative" program meant that RI Advice had failed to do all things necessary to ensure that financial services covered by its AFS licence were provided efficiently and fairly.

Order

RI Advice was ordered to engage cybersecurity experts to assess and advise on what more documentation and controls needed to be implemented in order to adequately manage cybersecurity risks. RI Advice has to implement such identified measures at the earliest reasonably practicable date, and to pay ASIC's costs.

Key Takeaways

AFS licence holders must manage cybersecurity risks and cyber resilience as part of their statutory obligations. Generally, company directors and senior officers should consider cyber resilience as part of their duties owed under the *Corporations Act*.

AFS licence holders should, in particular, take the following steps:

- Design and implement cybersecurity and cyber resilience regimes as quickly as possible, including a prompt and robust rectification of any identified deficiencies across their authorised representative network.
- Plan and implement an audit and monitoring program to audit and monitor on a regular basis the effectiveness of the implemented regime, including through the engagement of third party experts to independently verify that the regime has been effectively implemented.
- Where a cybersecurity incident occurs, undertake a post-incident review to determine whether the incident occurred as a result of a systemic issue with the compliance system or if some vulnerability was exploited.

Although the decision did not focus on the liability of individual directors for any cybersecurity inadequacies and only focused on the statutory obligations of AFS licence holders, ASIC has long stressed the important role of the board in ensuring companies are cyber resilient. Accordingly, company directors should take note of ASIC's role in bringing these proceedings and ensure that they diligently enquire of management about what steps are being taken to maximise cyber resilience in those companies.