A New 'Marker' for Cyber Security Practices
Implications of the RI Advice Group Decision

Alec Christie (Partner), **Avryl Lattin** (Partner), **Raeshell Staltare** (Special Counsel), **Christian Hofman** (Associate), **Alexia Psaltis** (Associate), Clyde & Co, comment on ASIC v RI Advice, the first case to address whether failing to manage cyber risk is a breach of financial services obligations and, possibly, directors' duties.

Introduction

On 5 May 2022, the Federal Court of Australia delivered its judgment in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* (***ASIC v RI Advice***) – the first case dealing with the issue as to whether failure to manage cyber risk is a breach of financial services obligations.

The Court made declarations that RI Advice Group Pty Ltd (**RI Advice**) had contravened its obligations as the holder of an Australian Financial Services Licence (**AFSL**) holder under sections 912A(1)(a) and (h) of the *Corporations Act 2001* (Cth) (**Corporations Act**) by failing to have appropriate cybersecurity controls and cyber resilience in place to manage its own cyber risks, and cyber risks across its network of authorised representatives (**ARs**).

Importantly, the Court emphasised that while there is a community expectation that reasonable cybersecurity measures are in place, the adequacy of cyber risk management must be determined by technical experts.

While the case focussed on the obligations of RI Advice as an AFSL holder, it nevertheless provides good general guidance for non-AFSL holders and directors of all companies as to how to best manage their own cyber risks to an acceptable standard

Background

ASIC v RI Advice was the first case brought by ASIC alleging that a failure to adequately manage cybersecurity risk is a breach by an AFSL holder of its core financial services obligations.

Although the matter was set down for trial in April 2022, RI Advice admitted a number of contraventions and the matter settled with the parties proposing declarations and orders to be made by consent with an agreed statement of facts (**SAFA**). Both parties filed submissions in support of the proposed declarations and orders.

Having considered the SAFA and the parties' submissions, Justice Rofe of the Federal Court considered there to be a proper basis for making the proposed declarations and orders in the form agreed by ASIC and RI Advice. In her Honour's reasons for judgment, she set out how AFSL holders should manage cyber risk. However, as we have noted, we believe that these reasons could equally apply to non-AFSL holders (in particular, company directors).

Key Takeaways from *ASIC v RI Advice*

- Cyber risk management is a highly technical area of expertise.
- The assessment of the adequacy of any particular cyber risk management systems requires the technical expertise of a relevantly skilled person.
- While there is an element of public expectation in the cyber standard, the relevant standard for the line management of cyber risk and associated controlled measures is not to be determined by reference to public expectation. It must be proportionate to the specific cyber risks facing the AFSL holder and its ARs as determined by technical experts. It could be inferred that the same might apply to non-AFSL holders, especially directors as regards the performance of their directors' duties particularly in relation to their company's cyber security generally.
- In the context of cyber risk management, the assessment of "adequate risk management systems" requires consideration of the risks faced by a business in respect of its operations and IT environment.
- It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level.
- Where cyber incidents occur, it is important that initiatives are taken quickly to improve cybersecurity and cyber resilience. Failure to implement necessary measures in a timely manner can constitute a breach of financial services obligations, or other more general obligations for non-AFSL holders (e.g. directors duties around cyber security).
- This case is the culmination of ASIC's focus on cybersecurity over the last 18-24 months. The emphasis on building cyber resilience is also in line with developments in other regulated sectors and the requirements foreshadowed by the critical infrastructure changes late last year and early this year.

Conduct of RI Advice

RI Advice is the holder of an AFSL under the Corporations Act. In turn, RI Advice also authorises and engages independent owned corporate and individual ARs to provide financial services to retail clients on RI Advice's behalf under its AFSL.

Between June 2014 and May 2020, various ARs of RI Advice experienced nine cybersecurity incidents.

Inquiries and reports made on behalf of RI Advice following the AR cyber security incidents revealed that there were a variety of concerns as regard the ARs' management of cyber security risks.

Admissions by RI Advice

In reaching a settlement with ASIC, RI Advice admitted that, prior to 15 May 2018, it did not have "adequate" cyber risk management systems (including documentation, controls and assurance) to manage cybersecurity risks across its ARs.

Although RI Advice made some significant improvements to its cybersecurity risk management systems including adopting a Cyber Resilience Initiative, RI Advice also admitted there should have had been a more robust implementation of cyber resilience prior to August 2021. It admitted that it "took too long to implement and ensure such measures were in place across its AR practices".

Overview of the decision

What is cybersecurity?

In the circumstances of RI Advice's financial services business, the Court defined cybersecurity as *"the ability of an organisation to protect and defend the use of cyberspace from attacks"* and cyber resilience as *"the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber sources."*

What is adequate cyber risk management?

While the Court did not go so far as to define specifically what AFSL holders must have in place to manage cyber risk (i.e., what is adequate in all cases), the decision does establish that a standard of care is required.

The Court rejected the suggestion that the relevant standard for assessment of adequate cyber risk management should be determined by "public expectation". The public is entitled to expect that appropriate cyber security measures are taken, the controls, measure and risk management relating to cybersecurity risk should not be assessed in this way.

Instead, the Court took the view that cyber risk management is a highly technical area of expertise and concluded that **"the assessment of the adequacy of any particular set of cyber risk management systems requires the technical expertise of a relevantly skilled person".**

As a guide to what is not adequate, this case provides the following examples:

- computer systems which did not have up-to-date antivirus software installed and operating;
- no filtering or quarantining of emails;
- no backup systems in place, or backups not being performed; and
- poor password practices including lack of multi-factor authentication, sharing of passwords between employees, use of default passwords, passwords and other security details being held in easily accessible places or being known by third parties.

Wide-ranging implications for organisations more broadly

It is important that all organisations consider the approach to cyber risk management and adequacy in light of this case. While this case was focussed on the obligations of AFSL holders, we expect that ASIC will also use its oversight powers to identify whether directors of any company that fails to adequately consider cyber risk, are in breach of their obligations.

Similarly, this decision is likely to inform the enforcement approach that other regulators take to cyber security issues. Those organisations that are required to comply with APRA's Prudential Standard CPS 234 – Information Security or which are affected by the new critical infrastructure requirements, should take note of this emerging standard for developing management of cyber risk.

On 5 May 2022, the date the ASIC v RI Advice judgment was delivered, ASIC's deputy chair, Sarah Court, made the following statement in relation to *ASIC v RI Advice*: *"ASIC strongly encourages all entities to follow the advice of the Australian Cyber Security Centre and adopt an enhanced cybersecurity position to improve cyber resilience in light of the heightened cyber-threat environment"*. This statement goes well beyond only AFSL holders and indicates ASIC's intention to promote this standard of cybersecurity across the board.

As the subject of multiple cyber incidents over an extended period, ASIC was successful in pursuing this test case on the question of cybersecurity expectations. From here, ASIC now has a benchmark with which it can pursue other entities, as observed by equivalent regulators in overseas jurisdictions.

By considering cybersecurity risk management a necessary investment, rather than an afterthought, organisations can avoid significant costs in the aftermath of an event. What started out as a series of IT issues ultimately escalated to becoming a high-profile ASIC prosecution involving legal compliance and reputational risk management issues.

In this case, RI Advice not only incurred costs in relation to the regulator investigation, responding to litigation and the remediation costs for uplifting their cyber security. In the absence of admissions made, if ASIC had to prove its case, the Court may have made additional orders including imposing significant penalties.

That being said, as risks relating to cybersecurity and the responsive measures to it are constantly evolving, organisations have an ongoing obligation to cast their minds to cybersecurity beyond initial setup. To ensure that this obligation is met, organisations should be conducting regular reviews of their infrastructure, ensuring that it is up to date and appropriate in the current circumstances.

This decision serves as a useful legal precedent for establishing a nexus between cybersecurity risk management and compliance with broader professional obligations. It may also form the basis of further precedent that applies across the professional services industry more broadly in terms of their own data handling and cyber security practices.