Where will the RI Advice proceedings take us?

AUGUST 2022

wotton kearney

A founding member of LEGALIGN GLOBAL

At a glance

- In August 2020, ASIC commenced proceedings against RI Advice for alleged breaches of its obligations as a financial services licensee under section 912A of the *Corporations Act 2001* (Cth) following numerous cyber incidents. ASIC and RI Advice reached an agreed settlement earlier this year.
- On 5 May 2022, the Federal Court delivered its penalty judgment. It made declarations of contraventions and ordered RI Advice to conduct a cybersecurity audit and to pay a contribution of $750,000 towards ASIC's costs.
- As the judgment relies on the facts agreed between ASIC and RI Advice as part of the settlement, relatively little weight can be placed on the findings. The market will take a keen interest in the cybersecurity standards courts seek guidance from when proceedings like this reach trial.
- While this is the first time ASIC has used its powers to enforce licensing obligations in a cyber context, it is not necessarily a watershed moment. These proceedings involved unusual circumstances, as RI Advice had experienced multiple cyber incidents over time.
- AFSL holders' approach to cyber risks will continue to be scrutinised as ASIC has just released its Corporate Plan for 2022-26, listing cyber risk and operational resilience as one of its core strategic projects. This includes taking enforcement action against failures to mitigate the risk of cyber attacks and related cyber resilience governance failures.
- In recent years, ASIC has attempted to take the 'stepping stone' approach to directors' liability off the back of contraventions by companies (an approach which has been the subject of competing judicial views). It remains to be seen whether ASIC attempts to take this route in the cybersecurity context as another way to shape corporate behaviour.

Background

In August 2020, in the first case of its kind, ASIC commenced proceedings against RI Advice Group Pty Ltd (RI Advice) for alleged failures surrounding the adequacy of RI Advice's cyber systems.

RI Advice provides financial services advice primarily through its network of Authorised Representatives (ARs). As a result, RI Advice holds an Australian Financial Services Licence (AFSL). RI Advice and its network have provided financial services to approximately 60,000 clients since May 2018.

RI Advice was impacted by nine cybersecurity incidents from June 2014 to May 2020. The impact of each incident was quite different and ranged from:

- business email compromises involving a relatively small number of clients' information
- the hacking of a client-facing website, which did not involve the compromise of any client personal information
- a ransomware incident affecting one device used for reception purposes
- a ransomware incident resulting in the loss of some client personal information, but not necessarily access or misuse of that information, and
- unauthorised access to a file server for several months, including the potential compromise of personal information of a significant number of clients.

These kinds of cyber attacks are very common and can target any company of any size or industry. It is important to note that the majority of the incidents that impacted RI Advice, based on the agreed statement of facts, did not have a significant impact on client personal information.

AFS licensees and section 912A of the *Corporations Act 2001* (Cth)

Under Australian financial services laws, the issuing, sale and distribution of certain financial products and the performance of financial services are subject to the AFSL regime under the *Corporations Act 2001* (Cth) (Corporations Act).

Section 912A of the Corporations Act contains 'general obligations' for AFS licensees, and the relevant obligations in the context of these proceedings were:[1]

Section	Obligation
912A(1)(a)	A financial services licensee must do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly.
912A(1)(h)	A financial services licensee must, subject to subsection (5)[2], … have adequate risk management systems.

Each of these sections, if contravened, constitutes a civil penalty provision. They carry significant financial penalties – up to $1m for an individual and potentially in the hundreds of millions for companies.

The allegations by ASIC and the admissions

While the pleadings comprised 175 pages detailing various cybersecurity incidents across RI Advice's AR network between June 2014 and May 2020, the penalty judgment was confined to a 12-page set of agreed facts (Agreed Facts).

RI Advice acknowledged in the Agreed Facts that before and on 15 May 2018, it did not have risk management systems that were adequate to manage risk regarding cybersecurity across its AR network. From May 2018 to August 2021, it made a series of improvements, such as engaging a forensic investigator, engaging a cybersecurity organisation to review a number of AR systems, and making a wide range of policies and programs to improve cybersecurity.

The Agreed Facts do not necessarily criticise RI Advice for the fact that cyber incidents occurred – which cannot always be prevented or avoided. Rather, the focus is on what RI Advice chose to do about the cyber incidents after they occurred and the time it took to implement the required security improvements. For example, RI Advice accepted "it should have had a more robust implementation of its program so that the measures were more quickly in place at each AR Practices and the majority of the AR network was confirmed as operating pursuant to such cybersecurity and resilience measures earlier".

What the Court said

The Court made the declarations sought – namely that RI Advice contravened s912A(1)(a) and (h) for the (seemingly agreed) period of 15 May 2018 to 5 August 2021. The Court's decision indicates that the security improvements should have been implemented more quickly following the nine cyber incidents. RI Advice was ordered to undergo a compliance program and contribute $750,000 to ASIC's costs. No civil penalty was ordered.

[1] ASIC also made allegations regarding other subsections within s912A, however the proceeding as settled concerned admitted breaches of 912(1)(a) and 912(1)(h) only.
[2] Which, in broad terms, exempts APRA-regulated bodies and RSE licensees from that obligation.

In issuing the penalty judgment, while the majority of the relevant facts and legal principles were agreed, the Court had to address what exactly providing financial services "efficiently" required in the context of 912A(1)(a) and, specifically, whether it requires a test of "public expectation".

The Court said that, in the context of cyber risk management, the relevant standard must be informed by people with technical expertise and not merely public expectation. While the public might have certain expectations about AFSL holders having adequate cybersecurity measures in place, the content of those measures must be assessed by reference to "the reasonable person qualified in that area, and likely the subject of expert evidence before the Court".

A watershed moment for ASIC cyber claims?

While there are learnings for insurers and insureds from the RI Advice proceedings, the outcomes are not necessarily a roadmap for future proceedings commenced by ASIC.

RI Advice's circumstances are unusual as it experienced numerous cyber incidents, some with more significant impacts on customers than others. Those circumstances, when considered with the facts that the outcome was agreed and not the subject of adjudication and that there was no civil penalty, suggest we will need to wait and see what ASIC's appetite is for future claims.

What cyber insurers and insureds can take from the proceedings is that a breach of s912A does not necessarily result from a cyber incident impacting a financial services provider. If a cyber incident does occur, regulators and courts will be particularly focussed on how a company responds in assessing and addressing vulnerabilities and the opinions of cyber experts regarding the adequacy of that response.

Time is critical when implementing cybersecurity measures, as is their regular review. Cybersecurity is not a 'set and forget' exercise. Insureds partnering with qualified experts will be helpful at the outset and when incidents occur to help manage the risk of claims by ASIC or other third parties.

ASIC's newfound cyber resilience focus – 2022-26 Corporate Plan & risks for directors

ASIC's newly released Corporate Plan for 2022-2026 makes clear that the scrutiny of ASIC-regulated entities' cybersecurity practices will be a core priority for the regulator.

With the ever-increasing risk of cyber attacks, and the significant impact they can have on consumers (from both service interruption and personal data risk standpoints), it is not surprising that ASIC is keen to drive good cyber risk and operational resilience practices in its regulated population.

ASIC has specifically flagged that it intends to take enforcement action against serious failures to mitigate the risks of cyber attacks and similar governance failures related to cyber resilience. As part of this strategic project, ASIC will be preparing a cross-industry self-assessment tool so ASIC-regulated entities can benchmark themselves against cyber resilience expectations.

The message from ASIC is for regulated entities to take cybersecurity seriously without delay. There are many ways ASIC may look to shift corporate behaviour in this way – one of which could be to attempt to use directors' personal culpability to drive change. ASIC has shown a propensity in the past to use enforcement action against a company as a basis to bring subsequent proceedings against directors and officers for a corresponding breach of duty of care. This has been described as a 'stepping stone' approach to liability, where ASIC uses a company's breach as a stepping stone to establishing personal breaches of care against directors and officers. It is a contentious approach but one which forms part of ASIC's litigation tool kit.

It is notable in this context that David Gonski has raised concerns about the vulnerability of directors to liability arising out of cyber incidents, as published in the AFR this month.

Mr Gonski noted that potential directors are in some instances turning down roles because of their concern about being personally culpable for cybersecurity failings and put forward the possibility of a 'safe harbour' style defence instead, as a way to offer relief and guidance about what the precise expectations of them are. The challenge with a safe harbour approach is that the question of what is reasonable in the context of adequate responses to cyber risks and threats has been the subject of little, if any, material guidance for businesses operating outside of essential services or critical infrastructure.

The RI Advice case is likely to be the first of several matters pursued by ASIC over inadequate cybersecurity. This is likely to extend beyond financial services to other sectors. The spectre of further regulatory activity by ASIC as it pursues its Corporate Plan, combined with the absence of regulatory or judicial guidance in respect of minimum cybersecurity standards, makes this a challenging area for directors and officers. This uncertainty inevitably creates risk and is an issue which insurers and insureds should be alive to so that it can be appropriately managed.

Need to know more?

For more information, please contact our authors.

Kieran Doyle
Partner, Sydney
Australian Cyber Leader
T: +61 2 8273 9828
kieran.doyle@wottonkearney.com.au

Cain Jackson
Partner, Melbourne
Financial Lines Practice Leader
T: +61 3 9604 7901
cain.jackson@wottonkearney.com.au

Jessica Chapman
Senior Associate, Sydney
T: +61 2 8273 9876
jessica.chapman@wottonkearney.com.au

Samantha Younane
Senior Associate, Melbourne
T: +61 3 9604 7941
samantha.younane@wottonkearney.com.au

wotton kearney

Get in touch with our specialists

W+K have dedicated cyber and D&O specialists across Australia and New Zealand, ready to assist with all your incident response, regulatory, policy coverage and claims needs.

Download our team contact cards below.