Australian
Banking & Finance
Law Bulletin

ASIC v RI Advice Group Pty Ltd — ASIC broadens its focus on defective systems

Felicity Healy *and* ***Camilla Bishop*** *CORRS CHAMBERS WESTGARTH*

Given heightened concerns about cybersecurity, it was only a matter of time before Australian Securities and Investments Commission (ASIC) sought out opportunities to create new laws on the adequacy of cybersecurity safeguards and the ability to protect consumers.

In the recent decision of *Australian Securities and Investments Commission (ASIC) v RI Advice Group Pty Ltd*[1] (*ASIC v RI Advice*), ASIC squarely brings this issue to the full attention of Australian financial services licence (AFSL) holders, and in particular, the need to ensure their authorised representatives (ARs) also have adequate systems in place to protect customers against cybersecurity threats.

As part of a court-approved settlement, RI Advice Group Pty Ltd admitted to a number of historical breaches of s 912A(1)(a) and (h) of the Corporations Act 2001 (Cth) which mostly related to the period prior to its acquisition by IOOF Holdings Ltd (now Insignia). Those breaches included failing to ensure that adequate cybersecurity measures were in place and/or adequately implemented across its ARs and failing to implement adequate cybersecurity measures thereby exposing the ARs' clients to an unacceptable level of risk.

Increased reliance on technology

Identifying defective systems is something ASIC is well versed in — albeit historically it has targeted defective systems through the lens of misleading or deceptive conduct. The focus of many of those claims was on representations made by a licensee that a customer would receive a particular benefit or service when in fact, the licensee's systems or processes were not equipped to deliver that benefit or service.[2] The *ASIC v RI Advice* decision demonstrates a desire by ASIC to broaden its focus to include other critical systems (such as cybersecurity and data protection systems) that may expose clients to an unacceptable level of risk.

ASIC has previously flagged the financial sector's increased reliance on technology throughout the pandemic as a trend to watch.[3] This reliance intensified during COVID-19 with licensees increasing their online presence and remote service offerings in response to consumer demand. Unsurprisingly, this coupled with widespread skills shortages have created a greater risk of cyberattacks and data breaches than ever before.

Need for technical expertise

It remains subject to debate as to whether the case successfully extended the operation of s 912A(1)(h), given that Rofe J agreed that it was not possible to reduce cybersecurity risk to zero, having regard to the parties' statement of agreed facts. However, given Rofe J's comments that assessment of the adequacy of cybersecurity systems is something that will require technical expertise, consideration of these kinds of issues is not something that should be postponed.

It is also unlikely that this will be ASIC's only foray into the adequacy of cybersecurity protections and it will be likely on the lookout for similar claims against AFSL holders who have not sought assistance from a relevantly skilled person to put in place proper controls. This is especially so considering that s 912A(1)(h) is a relatively recent civil penalty provision.

Perhaps another indicator of ASIC's focus on inadequate monitoring and compliance is the regulator's recent proceedings commenced against Macquarie Bank. In that case, ASIC alleges that Macquarie's "fee bulk transacting" system which was used by third parties, such as financial advisers, to bulk-process fees on multiple accounts exposed customers to a risk of fraudulent or unauthorised transactions. At the heart of ASIC's s 912A(1) claim is that, Macquarie had deficient systems in place to prevent or detect unauthorised transactions processed through the fee bulk transacting system.[4] What can be gleaned from these cases is that ASIC appears to be laser-focused on the control environment and the need for robust detection systems to identify and prevent harm from occurring. Further, ASIC will not necessarily wait until something has gone wrong before it commences an investigation.

Key points for AFSL holders

Although there could never be an expectation on AFSL holders to eliminate the risk of cybersecurity entirely, greater focus and scrutiny will be placed on the

adequacy of controls to identify and reduce risk and the need for clear documentation evidencing those steps.[5]

AFSL holders may reduce this risk by:

- considering whether there is adequate auditing or other compliance measures in place to ensure that ARs (and other representatives) operating under the AFSL holders are complying with any risk management systems (and that these risk management systems are well-documented). Examples of such systems include implementing multi-factor authentication and password-protecting sensitive material sent by email
- interrogating internal systems to ascertain whether there is a robust internal incident-monitoring process that captures potential defects in cybersecurity or data protection systems
- ensuring ARs (and other representatives) have adequate training and professional development events with respect to cybersecurity or data protection systems and
- considering engaging external cybersecurity experts early and staying on top of implementing processes and protocols that minimise risk to clients

Further guidance can also be found in the "three core initiatives" set out in the agreed facts of the *ASIC v RI Advice* case and steps taken in respect of each. There, the state of affairs that ASIC did and did not accept as a breach can be readily seen, albeit limited to the facts of that particular case.

Lastly, AFSL holders should also turn their minds to the recently extended breach reporting regime in light of this decision. While a breach of either s 912A(1)(a) or (h) of the Act would be a reportable situation under the new regime, frequently, such reportable situations will be hard to identify and care needs to be taken in terms of the timing of any internal investigation.[6]

Felicity Healy
Partner
Corrs Chambers Westgarth
felicity.healy@corrs.com.au
corrs.com.au

Camilla Bishop
Senior Associate
Corrs Chambers Westgarth
camilla.bishop@corrs.com.au
www.corrs.com.au

Footnotes

1. *Australian Securities and Investments Commission (ASIC) v RI Advice Group Pty Ltd* [2022] FCA 496; BC202203795.
2. See for example, *Australian Securities and Investments Commission (ASIC) v Commonwealth Bank of Australia* [2020] FCA 790; BC202004998.
3. Australian Securities and Investments Commission (ASIC) ASIC Corporate Plan 2020–24 Focus 2020–21 (2020) p 9.
4. Concise Statement, *Australian Securities and Investments Commission (ASIC) v Macquarie Bank Ltd* ACN 008 583 542.
5. Above n 1, at [58].
6. "Significant breaches" include breaches of a civil penalty provision which includes both s 912A(1)(a) and (h).