ASIC ENFORCEMENT ACTION SIGNALS INCREASING REGULATORY SCRUTINY OF DATA AND CYBER SECURITY PRACTICES

28 August 2020 | Australia
Legal Briefings – By **Tania Gray, Christine Wong and Tomas Kemmery**

ASIC has recently entered the fray on obligations of financial services providers to manage cyber risk, commencing proceedings against RI Advice Group.

WHAT DO THE PROCEEDINGS SHOW?

The proceedings are of interest because they show:

1. ASIC's appetite to take enforcement action against companies that fail to meet reasonable standards in managing cyber security risks. This reinforces that non-Privacy Commissioner regulators are taking direct data regulation action (the ACCC has already taken, and been successful in, actions for misuse of data by companies - our recent update on cases and fines here).

2. Possible divergences between regulatory expectations and what is happening in practice. The ASX release from RI's parent company, IOOF, states that the allegations relate to a small number of cyber-attacks "*of a nature not uncommonly faced by Australian businesses*".

3. Regulatory expectations that:

a. cyber security policies and procedures are appropriately tailored to the particular business (including any authorised representative (**AR**) network) and its risks; and

b. appropriate assessments and remedial steps are taken after incidents occur - ad hoc and discrete responses may not be sufficient.

Our cross-practice Cyber team can be contacted for further information.

WHAT IS ASIC ALLEGING?

ASIC's Concise Statement can be located here. In summary:

1. ASIC alleges that **RI failed to have and implement (including by its ARs) policies, procedures, controls and similar which were "reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience".** As a result, it breached its general obligations under s912A of the Corporations Act, including to:

a. provide services efficiently, honestly and fairly;

b. establish compliance measures to ensure compliance with financial services laws;

c. have adequate resources (financial, technological and human) to carry out supervisory arrangements; and

d. have adequate risk management systems.

2. As a result of this conduct, ASIC is seeking:

a. **Pecuniary penalties** (while those have been reported to be in the range of $12 million, any penalty will be determined by the court).

b. **Compliance orders** requiring RI to implement appropriate policies and procedures to manage cybersecurity risks, and to provide an independent expert report assessing its compliance with those orders.

The specific details of the allegations are as follows:

3. There were a **number of cyber breach incidents** at authorised individual and corporate ARs providing financial services on RI's behalf, including:

a. A ransomware attack in December 2016 on an AR which RI became aware of in early 2017.

b. In May 2017, the RI network was hacked, impacting 226 client groups.

c. For a period from late 2017 to early 2018, an unknown malicious agent spent more than 155 hours logged into a server, which was not detected for 3 months and resulted in 27 clients informing the AR of unauthorised use of their personal information and potentially 8,104 individuals exposed.

d. In May 2018, an unknown party obtained remote access to a system through a Trojan on a staff member's computer (which was again accessed in April 2020).

e. On about 23 August 2019, an unknown unauthorised party compromised a staff member's inbox.

4. It was **incumbent on RI in discharging its duties and functions as a licensee to have adequate systems, policies, procedures and controls in place to meet the reasonable standard that would be expected by the public** in appropriately

managing cybersecurity and cyber resilience risks across its AR network, particularly as ARs receive and store confidential and sensitive client information. RI failed to do this because:

a. The management of cyber security, including roles and responsibilities of RI and its ARs, was not adequately documented.

b. RI did not adopt and implement adequate and tailored cybersecurity documentation and controls in multiple cybersecurity domains (rather many of the documents were ANZ developed documents and not tailored to RIs requirements), such as governance and business environment, risk assessment and risk management.

c. RI should have taken a number of steps to improve its cyber security and cyber resilience after the particular incidents that occurred but did not, including: properly reviewing the effectiveness of controls and ensuring those were remediated in a timely manner; consulting with cybersecurity experts to promptly adopt a cybersecurity framework and undertaking a risk assessment across its entire AR network. While some discrete steps were taken, they were not part of an informed risk management framework and process.

4. The breaches have **caused harm** in the form of an unacceptable level of risk to RI, its ARs and their customers.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

PETER JONES

JULIAN LINCOLN

TANIA GRAY

MERRYN QUAYLE

PARTNER, SYDNEY

+61 2 9225 5588
peter.jones@hsf.com

PARTNER, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

PARTNER, SYDNEY

+61 2 9322 4733
Tania.Gray@hsf.com

PARTNER, MELBOURNE
+61 3 9288 1499
merryn.quayle@hsf.com

CHRISTINE WONG
SENIOR ASSOCIATE, SYDNEY
+61 2 9225 5475
Christine.Wong@hsf.com

LEGAL NOTICE