## Article Information

Author: Alasdair McLean
Service: Banking & Finance, Corporate & Commercial, Corporate & Commercial Finance, Cyber Security, Funds Management
Sector: Financial Services

# Fund FAQs – ASIC cybersecurity enforcement action against an AFSL holder

**ASIC announced on 21 August 2020 that it was commencing Federal Court proceedings against RI Advice Group Pty Ltd (RI), an Australian Financial Services Licence (AFSL) holder, in respect of alleged breaches of the Corporations Act 2001 (Cth) (Corporations Act) by failing to have adequate cyber security systems. This is one of the first times that ASIC has taken this type of action and it is a clear sign of the regulator's increased focus on cybersecurity and cyber resilience. It is a timely reminder of the broad scope of obligations that are imposed on licensed entities and the increasing need to actively engage on cyber security risks as part of an AFSL holder's compliance framework.**

*The allegations*

ASIC's action follows a number of alleged cyber breach incidents by certain authorised representatives of RI, including an alleged cyber breach incident at Frontier Financial Group Pty Ltd as trustee for The Frontier Trust (**Frontier**) over a 6 month period in late 2017 to early 2018. One of ASIC's allegations is that Frontier was subject to a 'brute force' attack that resulted in an unauthorised user gaining remote access to Frontier's database of sensitive client information for more than 155 hours.

After becoming aware of the breach at Frontier, and with knowledge of other cybersecurity incidents within its authorised representative network, ASIC alleges that RI contravened key provisions of the Corporations Act by failing to maintain adequate policies, systems and resources to manage risk in respect of cybersecurity and cyber resilience. These obligations arise as part of the requirements under the Corporations Act that an AFSL holder:

- does all things necessary to ensure that the financial services covered by its licence are provided efficiently, honestly and fairly;
- complies with the financial services laws;
- takes reasonable steps to ensure that its authorised representatives comply with the financial services laws;
- has adequate resources (including financial, technological and human resources) to provide the financial services covered by its licence and to adequately supervise the arrangements in place; and
- puts in place adequate risk management systems.

ASIC is seeking declarations that RI contravened various provisions of the Corporations Act, pecuniary penalty orders, and compliance orders that RI implements systems that are reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience (which ASIC is seeking to have confirmed by an independent expert report once implemented).

*Compliance risks*

It is recommended that all AFSL holders undertake a regular 'health check' of their risk assessments, and the measures that they have in place to mitigate or avoid those risks. In this regard, cyber risks are obviously an increasing risk for all financial service providers. As ASIC has previously identified, an adequate risk management system will need to:

- be based on a structured and systematic process that takes into account the key risks to the AFSL holder's business in light of its obligations under the Corporations Act;
- focus in particular on risks that adversely affect consumers or market integrity;
- establish and maintain controls designed to manage or mitigate those risks; and
- fully implement and monitor those controls to ensure they are effective.

A regular review of the adequacy of an AFSL holder's technological resources, including IT system security, disaster recovery systems and business recovery is another important component of an effective risk management system. The case against RI also evidences the importance of implementing appropriate steps to respond adequately when cybersecurity incidents reveal gaps in an entity's risk managements systems and resources, including in relation to its authorised representative network.

For responsible entities, the disclosure of any identified cyber risks will need to be carefully considered in any product disclosure statement that is published.

Finally, all AFSL holders need to be conscious of their breach reporting obligations in the event that a cybersecurity breach is identified.