ASIC Targets AFS Licensees with Inadequate Cyber Security

Posted by Cowell Clarke Financial Services Team 24 August 2020

AFS Licensees should be aware that ASIC are actively pursuing Licensees that have inadequate cyber security systems.

On 21 August, ASIC launched Federal Court proceedings against AFS Licensee RI Advice Group Pty Ltd (**RI Advice**) based on its alleged failure to have adequate cyber security systems or to appropriately rectify the data breaches.

ASIC has alleged that multiple authorised representatives (**AR**) of RI Advice had cyber security breaches.

In particular, ASIC alleges that a substantial cyber breach incident occurred at an AR of RI Advice, Frontier Financial Group Pty Ltd (**Frontier**), between December 2017 and May 2018. ASIC has alleged that the malicious agent that breached Frontier's server spent more than 155 hours logged into a server that contained sensitive client identification documents. By 31 July 2018, 27 Frontier clients had informed Frontier of the unauthorised use of their personal information.

ASIC alleges RI Advice failed to implement adequate policies, systems and resources which were reasonably appropriate to manage cyber security risks and cyber resilience to implement adequate policies, systems and resources which were reasonably appropriate to manage cyber security risks and cyber resilience.

ASIC is seeking declarations that that RI Advice breached its obligations as an AFS Licensee and contravened ss 912A(1)(a), (b), (c), (d) and (h) and (5A) of the *Corporations Act 2001* (Cth), which includes the legal obligations to:

- Do all things necessary to ensure that financial services are provided efficiently, honestly and fairly.
- Comply with conditions on the AFSL (which include that the Licensee must establish and maintain compliance measures).
- Have adequate resources (including technological) to provide financial services and supervise representatives.
- Have adequate risk management systems.

ASIC is seeking civil penalties and compliance orders.

The action comes at a time where AFS Licensees may be exposed to heightened cyber security risks due to flexible work environments as a result of the COVID-19 pandemic.

We recommend that all Licensees regularly review their cyber security policies and systems to ensure that their clients' data remains secure and confidential. Failure to provide adequate measures to protect against malicious software can lead to ASIC enforcement and legal action.

If you need any assistance with cyber security policies as an AFS Licensee, or in monitoring the practices of your ARs, please do not hesitate to get in contact with a member of the Financial Services Team.