“Have you tried turning it off and on again?” – A review of the decision in ASIC V Ri Ad

25 May 2022
From The Fold Legal

Simon Carrodus

On 5 May 2021, the Federal Court handed down a landmark decision in Australian Securities and Investments Commission v RI Advice Group Pty Ltd (2022) FCA 496 by declaring that RI Advice Group Pty Ltd (RI Advice) had breached its obligation to:

1. provide financial services efficiently, honestly, and fairly, and
2. have in place adequate risk management systems, by failing to have adequate cybersecurity risk management controls in place. This was a landmark decision as it was the first time that an AFS licensee had been found to be in breach of the requirement for AFS licensees to provide financial services efficiently, honestly, and fairly by not having adequate cybersecurity risk management systems.

In this article, we explore:

1. What happened?
2. What did the Court say?
3. What does this mean for AFS licensees?
4. How The Fold can help.

What Happened?

RI Advice, as the AFS licensee of more than 100 authorised representative (AR) practices, provided financial services to approximately 60,000 retail clients.
Between June 2014 and May 2020, a number of separate cybersecurity incidents occurred at the AR practices. These cybersecurity incidents involved:

1. the hacking of an AR practice's Google email account
2. the hacking of an AR practice's third party website provider (which hosted the AR practice's knowledge centre)

3. a hacker sent an email to a client, from the email address of an employee of the AR practice, requesting money
4. an AR practice's reception desk computer being subject to ransomware delivered by email, resulting in certain files being encrypted and made inaccessible
5. an AR practice's server being hacked by brute force through a remote access port, resulting in files being held ransom and 220 client files becoming encrypted and unrecoverable
6. an AR practice being hacked through brute force and being undetected for several months, resulting in thousands of client files becoming compromised and personal information stolen – this also resulted in phishing emails being sent to clients
7. the hacking of an AR practice's email and an email being sent to the AR practice's bookkeeper requesting that funds be transferred to a Turkish bank, and
8. the hacking of an employee of an AR practice's email resulting in 150 phishing emails being sent to the AR practice's clients requesting that they access a Dropbox folder.

While RI Advice had organised some cyber security training sessions for its ARs and had implemented some information security controls s, RI Advice conceded that these steps were inadequate to manage its cyber security risk across its AR practices.
It was also identified that at one particular AR practice up to 90% of the desktops did not have up to date anti-virus software, no scans were scheduled during the week for antivirus software, no offsite backup had been performed and password and security details were found in text files on the server desktop.
In June 2018, RI Advice engaged cyber security consultants and independent experts to investigate specific incidents and to identify and implement measures to address cybersecurity risks. RI Advice also updated its cyber security policies and introduced measures that required its authorised representatives hold cyber insurance. However, RI Advice but admitted that it took too long to implement these measures across its practices.
On 21 August 2020, ASIC commenced proceedings against RI Advice for an alleged failure to:

1. provide financial services efficiently, honestly, and fairly
2. comply with the conditions of its AFS licence
3. comply with financial services laws, and
4. have available adequate resources provide the financial services and carry out supervisory arrangements.

ASIC and RI Advice ultimately settled the matter, with RI Advice admitting to the Court on 7 April 2022 that it had contravened its obligations to:

1. provide financial services efficiently, honestly, and fairly, and
2. have in place adequate risk management systems.

What did the Court say?

Efficiently, honestly, fairly

Although RI Advice admitted to contravening section 912A(1)(a) of the Corporations Act, it disagreed with ASIC's argument regarding what was the appropriate test for determining whether a breach of this section had occurred. RI Advice argued that the "public expectation" test (as submitted by ASIC) was not the appropriate test for determining whether an AFS licensee had breached the efficiently, honestly, and fairly obligation.
Justice Rofe agreed with RI Advice, stating that:
"In a technical area such as cybersecurity risk management, the reasonable standard of performance is to be assessed by reference to the reasonable person qualified in that area, and likely the subject of expert evidence before the Court, not the expectations of the general public".
RI Advice also argued that, while they admitted to contravening the efficiently, honestly, and fairly provision, it did not mean that they had not acted "honestly".
Justice Rofe agreed with RI Advice stating that a party could contravene the efficiently, honestly, and fairly obligation without having acted dishonestly.

Adequate risk management systems

RI Advice also admitted to contravening the requirement under the Corporations Act to have in place adequate risk management systems. Justice Rofe provided some guidance around what constituted "adequate risk management systems".
On the question of "adequacy", her Honour clarified that the Court's assessment of adequate risk management systems (including those of AFS licensee) will be informed by evidence from relevantly qualified experts in the field.

Outcome

As a result of RI Advice admitting to contravening sections 912A(1)(a) and (h) of the Corporations Act, the Court ordered that RI Advice must:

1. Engage a cybersecurity expert to identify what further documentation and controls in respect of cybersecurity and cyber resilience are necessary for RI Advice to manage risk across its AR practices, and
2. Pay $750,000 towards ASIC's costs.

What does this mean for AFS licensees?

The RI Advice case clarifies that each AFS licensee must have in place cybersecurity risk management systems across their AR network to protect themselves and their clients from cybersecurity attacks. This includes:

1. up-to-date anti-virus software
2. regular virus scans across the whole AR network
3. up-to-date cybersecurity and cyber resilience training for directors, employees and ARs
4. an AFS licensee cybersecurity policy which ARs are required to implement and comply with as a part of their AR agreement. The cybersecurity policy should address:
    1. Data protection
    2. Password protection and storage, and
    3. Process for dealing with spam and suspected phishing emails.

This case also makes it abundantly clear that the cyber resilience of an AFS licensee's AR network is the responsibility of the AFS licensee and not the individual AR practice. Determining whether a breach of your AFS licensee obligations requires technical knowledge and expertise in cybersecurity.

How The Fold can help

If you are concerned that your cybersecurity risk management systems and policies may not be adequate, we are here to help.
Through our relationship with some of the best cybersecurity firms in Australia, The Fold Legal can conduct a coordinated cybersecurity health check. We will:
1. Update or create your cybersecurity and cyber resilience policies;
2. Conduct cybersecurity penetration tests of your risk management systems;
3. Provide advice on any identified cybersecurity breaches and how they impact your AFS licensee obligations; and
4. Conduct a full cybersecurity review to ensure that you are running a "best-in-practice" AFS licensee business.

By Simon Carrodus and Glenjon Aligiannis.

https://www.adviservoice.com.au/2022/05/have-you-tried-turning-it-off-and-on-again-a-review-of-the-decision-in-asic-v-ri-ad/