NOTICE OF FILING

This document was lodged electronically in the FEDERAL COURT OF AUSTRALIA (FCA) on 21/08/2020 7:52:05 AM AEST and has been accepted for filing under the Court's Rules. Details of filing follow and important additional information about these are set out below.

Details of Filing

Document Lodged:	Concise Statement
File Number:	VID556/2020
File Title:	AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION v RI ADVICE GROUP PTY LTD (ACN 001 774 125)
Registry:	VICTORIA REGISTRY - FEDERAL COURT OF AUSTRALIA

Dated: 21/08/2020 8:51:40 AM AEST Registrar

Important Information

As required by the Court's Rules, this Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

The date and time of lodgment also shown above are the date and time that the document was received by the Court. Under the Court's Rules the date of filing of the document is the day it was lodged (if that is a business day for the Registry which accepts it and the document was received by 4.30 pm local time at that Registry) or otherwise the next working day for that Registry.

Form NCF1

Concise Statement

No. of 2020

Federal Court of Australia

District Registry: Victoria

Division: General

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION

Plaintiff

RI ADVICE GROUP PTY LTD (ACN 001 774 125)

Defendant

A IMPORTANT FACTS GIVING RISE TO THE CLAIM

Introduction

1 The Defendant (**RI**) holds Australian financial services licence number 238429 (**AFSL**) and is a financial services licensee within the meaning of the *Corporations Act 2001* (Cth) (**Act**). The AFSL requires RI to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that RI complies with the provisions of the financial services laws.

2 Until 1 October 2018, RI was a wholly owned subsidiary of Australia and New Zealand Banking Group Limited (**ANZ**). On 1 October 2018, RI became a wholly owned subsidiary of IOOF Holdings Limited (**IOOF**) and a member of the **IOOF Group** (comprising IOOF and its subsidiaries).

3 RI has authorised individual and corporate authorised representatives (**ARs**) to provide financial services on its behalf. RI's ARs receive and store, electronically, confidential and sensitive client information and documents, including relating to financial matters. It therefore was and is incumbent on RI in discharging its duties and functions as a licensee to have adequate systems, policies, procedures and controls in place that met and meet the reasonable standard that would be expected by the public in appropriately managing risks in relation to cybersecurity and cyber resilience across its AR network.

4 As at 15 May 2018, RI had 286 ARs, comprising 192 individuals and 94 corporate entities. As at 1 May 2020, RI had 293 ARs, comprising 191 individuals and 102 corporate entities.

Cybersecurity incidents in 2016/2017 at Wise Financial Planning and RI Circular Quay

5 On about 3 January or 3 March 2017, RI became aware of a cybersecurity incident involving its then AR, Anthony Hilsley, who was a financial adviser and principal and director of Superannuation Advisory Service Pty Ltd trading as Wise Financial Planning. RI was

Filed on behalf of (name & role of party)	The Plaintiff
Prepared by (name of person/lawyer)	Andrew Christopher
Law firm (if applicable)	Webb Henderson
Tel +61 2 8214 3510	Fax N/A
Email Andrew.Christopher@webbhenderson.com	
Address for service (include state and postcode)	Webb Henderson, Level 18, 420 George St, Sydney NSW 2000 Andrew.Christopher@webbhenderson.com

informed that, in about late December 2016, Wise Financial Planning's main reception computer was hacked by ransomware, which encrypted files and made them inaccessible.

6 On 30 May 2017, RI became aware of a cybersecurity incident that day involving its AR, John Leslie Walker, who is a financial adviser and principal of RetireInvest Circular Quay (**RI Circular Quay**). RI was informed that RI Circular Quay's local network was hacked through a remote access port, impacting about 226 client groups.

7 After becoming aware of each of the cybersecurity incidents referred to in paragraphs 5 and 6 above, RI should have, but failed to: (a) properly review the effectiveness of cybersecurity controls relevant to these incidents across its AR network, including account lockout policies for failed log-ins, password complexity, multi-factor authentication, port security, log monitoring of cybersecurity events, cyber training and awareness, email filtering, application whitelisting, privilege management and incident response controls; and (b) ensure that those controls were remediated across its AR network where necessary in a timely manner, in order to adequately manage risk with respect to cybersecurity and cyber resilience.

Cybersecurity incident between December 2017 and April 2018 – the FFG breach

8 From about 30 December 2017 until about 15 April 2018, an unknown malicious agent obtained and retained unauthorised remote access to the file server of RI's AR, Frontier Financial Group Pty Ltd as trustee for The Frontier Trust (**FFG**) (**FFG breach**), through an FFG employee's account. The malicious agent spent more than 155 hours logged into the server, which contained sensitive client information including identification documents. FFG did not detect the FFG breach until 16 April 2018, more than 3 months after it had commenced. On 15 May 2018, FFG informed RI of the FFG breach, and that 3 clients had informed FFG of the unauthorised use of their personal information, which included a mail redirection application being lodged with Australia Post and multiple bank accounts being opened without their consent. On 4 June 2018, FFG lodged a Notifiable Data Breach form with the Office of the Australian Information Commissioner (**OAIC**). By 31 July 2018, 27 clients had informed FFG of the unauthorised use of their personal information. On 19 September 2019, FFG informed the OAIC, and RI was aware, that FFG's investigation had revealed that there were 8,104 individuals potentially exposed to the FFG breach.

RI's risk management systems and resources with respect to cybersecurity and cyber resilience prior to and as at 15 May 2018 were inadequate

9 Prior to and as at 15 May 2018, RI held minimal and inadequate documentation for the management of cybersecurity and cyber resilience across its AR network. The roles and responsibilities of RI and its ARs as to the management of cybersecurity risk and cyber resilience were not documented. Many cybersecurity documents were ANZ-developed documents specific to the ANZ organisation and its IT environment, and were not tailored to RI and its ARs' requirements. RI and its ARs had not implemented and operationalised these ANZ-developed documents as part of RI's governance and management of cybersecurity resilience and risk management. RI did not adopt and implement adequate and tailored cybersecurity documentation and controls in each of the following cybersecurity domains: governance and business environment, risk assessment and risk management, asset

management, supply chain risk management, access management, personnel security training and awareness, data security, secure system development life cycle and change management, baseline operational security, security continuous monitoring, vulnerability management, incident response and communication, and continuity and recovering planning. Accordingly, RI's risk management systems and resources with respect to cybersecurity and cyber resilience prior to and as at 15 May 2018 were inadequate.

Cybersecurity incident in May 2018 at RI Shepparton

10 On about 29 May 2018, RI became aware of a cybersecurity incident on 23 May 2018 involving its ARs, Sandra Miller and Financial Lifestyle Partners (Shepparton) Pty Ltd (**RI Shepparton**). RI was informed that an unknown party had obtained unauthorised access to Sandra Miller's RI Shepparton email account and used the account to request a bookkeeper to transfer funds to a Turkish bank account (which transfer was not made). In about July 2018, RI was informed that a third-party information technology (**IT**) service provider had reviewed the incident and had concluded that the likely cause was a Trojan (a form of malicious software) installed on Sandra Miller's laptop computer.

Following the FFG breach, the Vixtro report, CARRs and KPMG forensic report identified significant cybersecurity gaps

11 On about 7 August 2018, FFG provided RI with a report prepared by a third-party IT service provider, Vixtro, which identified a number of deficiencies with FFG's desktop and network security. The reported deficiencies included 90% of desktops identified as not having up to date antivirus software, no filtering or quarantining of emails, no offsite backups having been performed and passwords and other security details found in text files on the server desktop.

12 In about September 2018, RI engaged Security in Depth, a third-party cybersecurity firm, to perform a cyber assurance risk review (**CARR**) of five ARs, including RI Circular Quay and RI Shepparton. Between September and October 2018, RI was provided with five CARR reports, rating three ARs' cybersecurity status as 'Poor' (including RI Circular Quay and RI Shepparton), and two ARs' cybersecurity status as 'Fair'. In relation to the three ARs rated as 'Poor', the CARR reports noted that the ARs had no discernible cybersecurity policies, processes and procedures in writing, and no structured security governance program driven from the executive down, and that it was highly likely that a cyber incident could occur over the next 12 months with significant impact on the ARs' ability to provide critical services. Security in Depth recommended in a further October 2018 report to RI that RI immediately have CARRs performed of all of its AR organisations. RI did not implement such a review.

13 On about 24 October 2018, KPMG provided RI with a report setting out its conclusions and recommendations from its investigation of the FFG breach. KPMG concluded that the FFG breach was likely to be the result of a brute force attack using an FFG employee login, as between 20 and 30 October 2017 there were 27,814 unsuccessful login attempts using 2,178 different user names from 10 different countries. KPMG reported that the malicious agent had installed various software on the FFG server including to enable brute forcing, crypto currency mining, a virtual private network, peer-to-peer file sharing and other hacking capability. It was reported that the malicious user had access through the compromised FFG user's account to

the entire contents of FFG's file server. KPMG recommended that, as a baseline, FFG should consider implementing the Australian Cyber Security Centre's Essential Eight cybersecurity strategies to mitigate cybersecurity incidents, and that after this was implemented a review of FFG's information security posture should be conducted, including a vulnerability assessment and penetration testing in order to understand and manage the ongoing risk profile.

The steps taken by RI in 2018 and 2019 following the FFG breach were inadequate

14 After becoming aware of the FFG breach, and with knowledge of the Wise Financial Planning, RI Circular Quay and RI Shepparton cybersecurity incidents, and the reports referred to in paragraphs 11 to 13 above, RI should have, in consultation with internal or external cybersecurity experts, promptly adopted a cybersecurity framework to guide all of its cyber-related activities, undertaken a risk assessment across its entire network of ARs, and then sought technical security assurance across a number of its ARs as a technical measure of the cybersecurity risks that exist in their organisations. Armed with this information, it should then have analysed the results to determine the current cybersecurity risks applicable to its network of ARs, and then developed and implemented a cybersecurity remediation plan and supporting initiatives that were tailored to its AR network. RI should have implemented reasonably sufficient and appropriate steps to adequately manage risk in respect of cybersecurity and cyber resilience across its AR network, and could and should have done so by no later than 30 September 2019. As referred to in paragraph 15 below, RI did not do this, and the steps which it did take were neither timely nor sufficient.

15 After October 2018, RI planned and undertook a number of discrete cybersecurity initiatives with the stated intention of addressing cybersecurity across its AR network, but it did not take these steps as part of an informed risk management framework and process of the type referred to in paragraph 14 above. Further, following the change of ownership of RI from ANZ to IOOF, RI replaced ANZ-developed documentation relating to cybersecurity with IOOF-developed documentation which often pre-dated IOOF's acquisition of RI. Like the ANZ documents, the IOOF documents were not tailored to RI and its ARs' requirements, and RI and its ARs did not implement and operationalise them as part of RI's own governance and management of cybersecurity resilience and risk management. RI's risk management systems and resources with respect to cybersecurity and cyber resilience remained inadequate, including as at 12 March 2019.

Cybersecurity incident in August 2019 at Empowered

16 On about 23 August 2019, RI became aware of a cybersecurity incident that month involving its then AR, Empowered Financial Partners Pty Ltd (**Empowered**). RI was informed that an external IT service provider had investigated the incident and ascertained that an unauthorised party had compromised an Empowered staff member's mailbox account. Following this incident, RI should have, but failed to: (a) properly review the effectiveness of cybersecurity controls relevant to this incident across its AR network, including cyber training and awareness, multi-factor authentication including of email accounts, incident response and email filtering controls; and (b) ensure that those controls were remediated across its AR network where necessary in a timely manner, in order to adequately manage risk with respect

to cybersecurity and cyber resilience. Accordingly, the steps taken by RI in relation to cybersecurity as a consequence of the Empowered incident were inadequate.

RI's risk management systems and resources with respect to cybersecurity and cyber resilience remained inadequate as at 1 November 2019

17 The steps taken by RI in relation to cybersecurity in the period from 15 May 2018 to 1 November 2019 were neither initiated nor completed in a sufficiently timely manner, and were not sufficiently broad. RI's risk management systems and resources with respect to cybersecurity and cyber resilience remained inadequate, including as at 13 March 2019 and 1 November 2019. As at 1 November 2019, RI had still not adopted and implemented adequate and tailored cybersecurity documentation and controls in each of the cybersecurity domains referred to in paragraph 9 above, and much of its cybersecurity documentation comprised IOOF-developed documents which suffered from the types of deficiencies identified in paragraph 15 above.

Cybersecurity incident in April 2020 at RI Shepparton

18 On about 15 April 2020, RI became aware of a cybersecurity incident that month which, for the second time, involved an external party's unauthorised use of Sandra Miller's RI Shepparton email account. On about 19 May 2020, RI was provided with a further CARR report dated April 2020 which rated RI Shepparton's cybersecurity status as still 'Poor'. The report identified that the cause of the second RI Shepparton incident was a suspected phishing attack, and that the unknown party had monitored the RI Shepparton email account for a period of time and had access to thousands of email addresses and contact details, as well as over ten thousand emails. The report highlighted a number of significant cybersecurity issues, including the poor level of password security and no utilisation of two factor authentication.

RI's risk management systems and resources with respect to cybersecurity and cyber resilience were still inadequate as at 1 May 2020

19 The steps taken by RI in relation to cybersecurity in the period from 1 November 2019 to 1 May 2020 were neither initiated nor completed in a sufficiently timely manner, and were not sufficiently broad. RI's risk management systems and resources with respect to cybersecurity and cyber resilience remained inadequate, including as at 1 May 2020. As at 1 May 2020, RI had obtained up-to-date cyber resilience assessments for only 3 of RI's AR practices, and reported to the plaintiff that only 34 RI practices had attested to the implementation of all elements within RI's recently revised Cyber Security Support Guide, and that RI did not expect to have implemented its strategy for the management of cybersecurity risk and resilience until the end of 2020. RI had still not adopted and implemented adequate and tailored cybersecurity documentation and controls in each of the cybersecurity domains referred to in paragraph 9 above, and much of its cybersecurity documentation remained IOOF-developed documents which suffered from the types of deficiencies identified in paragraph 15 above.

B SUMMARY OF RELIEF SOUGHT FROM THE COURT

20 As set out in the Originating Process, the plaintiff seeks declaratory relief under s 21 of the *Federal Court of Australia Act 1976* (Cth) and/or ss 1101B(1)(a) and 1317E of the Act, pecuniary penalty orders under s 1317G(1)(a) of the Act, compliance orders under s 1101B(1)(a) of the Act and costs.

C PRIMARY LEGAL GROUNDS FOR THE RELIEF SOUGHT

21 By reason of the matters referred to above, and as set out in the Originating Process, RI has breached its obligations as a financial services licensee and contravened ss 912A(1)(a), (b), (c), (d) and (h) and (5A) of the Act.

D HARM SUFFERED

22 It is essential that an AFSL holder such as RI, which holds (including by its ARs) confidential and sensitive client information and documents, has in place adequate risk management systems, and resources (including technological and other resources), in respect of cybersecurity and cyber resilience. The contraventions of the statutory provisions by reason of the matters referred to above have given rise to an unacceptable level of risk to RI, its ARs and their customers, of cybersecurity incidents and consequential effects.

Certificate of lawyer

I, Andrew John Christopher, certify to the Court that, in relation to the concise statement filed on behalf of the plaintiff, the factual and legal material available to me at present provides a proper basis for each allegation in the pleading.

Date: 21 August 2020

Signed by Andrew John Christopher

Lawyer for the plaintiff

This concise statement was prepared by Fleur Shand of counsel and settled by Stephen Parmenter QC and Paul Liondas of counsel.