NOTICE OF FILING

This document was lodged electronically in the FEDERAL COURT OF AUSTRALIA (FCA) on 20/10/2021 1:57:00 PM AEDT 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:	Statement of Claim - Form 17 - Rule 8.06(1)(a)
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: 21/10/2021 2:04:35 PM AEDT 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.

No. VID 556 of 2020

Form 17
Rule 8.05(1)(a)

Second Further Amended Statement of Claim

(Filed pursuant to orders made on 5 October 2021)

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

TABLE OF CONTENTS

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 Ref
Address for service (include state and postcode) Webb Henderson, Level 18, 420 George St, Sydney NSW 2000
Andrew.Christopher@webbhenderson.com

[Form approved 01/08/2011]

A. THE PARTIES AND THE AUTHORISED REPRESENTATIVES

1 The plaintiff (**ASIC**) is:

(a) a body corporate under s 8(1)(a) of the *Australian Securities and Investments Commission Act 2001* (Cth) (the **ASIC Act**); and

(b) entitled to commence and maintain this proceeding in its corporate name under s 8(1)(d) of the ASIC Act.

2 The first defendant (**RI Advice**):

(a) at all material times up to and including 30 September 2018 was a wholly-owned subsidiary of Australia and New Zealand Banking Group Limited (**ANZ**);

(b) was one of three ANZ aligned dealer groups (**Aligned Dealer Groups**) which from 1 October 2018 became part of the IOOF Holdings Limited (**IOOF**) group of companies;

(c) since 1 October 2018 has been a wholly-owned subsidiary of IOOF;

(d) is and at all material times was the holder of Australian Financial Services Licence (**AFSL**) number 000238429 (**Licence**) and a financial services licensee (within the meaning of s 761A of the *Corporations Act 2001* (Cth) (the **Act**)); and

(e) is and at all material times was carrying on a financial services business (within the meaning of s 761A of the Act), including by providing financial product advice (within the meaning of s 766B of the Act) to retail clients (within the meaning of s 761G of the Act) (**Retail Clients**) through authorised representatives (within the meaning of s 761A of the Act) (**ARs**) who provided financial services on RI Advice's behalf pursuant to s 916A of the Act.

3 At all material times, in the course of providing financial services on RI Advice's behalf, RI Advice's ARs received and stored and accessed, electronically, confidential and sensitive personal information and documents in relation to Retail Clients (**Personal Information**), including:

(a) personal details, including full names, addresses and dates of birth;

(b) contact information, including contact phone numbers and email addresses;

(c) copies of identification documents, such as driver's licenses, and passports;

(d) tax file numbers; and

(e) bank account and credit card details and other financial information.

4 Since 15 May 2018, RI Advice's ARs have provided financial services on RI Advice's behalf to approximately 60,000 Retail Clients.

Particulars

RI Advice website: "Become an adviser"
www.riadvice.com.au/become-an-adviser -
(accessed on 22 October 2020).

5 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 and 4 above, at all material times, RI Advice and each of its ARs were potential targets for cyber-related attacks and cybercrime by malicious actors targeting Personal Information.

6 As at 15 May 2018, RI Advice had 270 ARs, comprising:

(a) 176 individual ARs; and

(b) 94 corporate ARs.

7 As at 12 and 13 March 2019, RI Advice had 283 ARs, comprising:

(a) 198 individual ARs; and

(b) 85 corporate ARs.

8 As at 1 November 2019, RI Advice had 297 ARs, comprising:

(a) 198 individual ARs; and

(b) 99 corporate ARs.

9 As at 1 May 2020, RI Advice had 293 ARs, comprising:

(a) 191 individual ARs; and

(b) 102 corporate ARs.

10 At all material times, since 15 May 2018:

(a) RI Advice's AR's have provided financial services on RI Advice's behalf organised in practices of groups of one or more ARs (**RI Advice Practices**); and

(b) there have been between about 89 and 110 RI Advice Practices.

Particulars

The RI Advice website contains a list of RI Advice Practices: www.riadvice.com.au/find-an-adviser (accessed on 26 October 2020).

As at 10 August 2018, there were 110 RI Advice Practices: email from Peter Ornsby, CEO of RI Advice, to Michael Connory, CEO of Security in Depth, dated 10 August 2018 [RIF.0004.0004.3598].

As at 1 May 2020, RI Advice stated that there were 89 RI Advice Practices: Letter from RI Advice to ASIC dated 1 May 2020 [FFG.1027.0001.0003].

B. OBLIGATIONS TO IMPLEMENT ADEQUATE CYBERSECURITY SYSTEMS

11 At all material times, RI Advice was required to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that RI Advice complies with the provisions of the financial services laws.

Particulars

Clause 2 of the Licence.

12 At all material times, as the holder of the Licence, RI Advice was required:

(a) pursuant to s 912A(1)(a) of the Act, to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly;

(b) pursuant to s 912A(1)(b) of the Act, to comply with the conditions on the Licence (including clause 2 of the Licence);

(c) pursuant to s 912A(1)(c) of the Act, to comply with the financial services laws (which included s 912A(1)(a), (b), (d) and (h) of the Act);

(d) pursuant to s 912A(1)(d) of the Act, to have available adequate resources (including financial, technological, and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements; and

(e) pursuant to s 912A(1)(h) of the Act, to have adequate risk management systems.

13 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 and 12 above, at all material times, RI Advice was required to:

(a) identify the risks that it and its ARs faced in the course of providing financial services on RI Advice's behalf, including in relation to cybersecurity and cyber resilience; and

Particulars

Cybersecurity is the ability to protect and defend the use of cyberspace from attacks.

Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources regardless of the source.

(b) have strategies, frameworks, policies, plans, procedures, standards, guidelines, systems, resources and controls in respect of cybersecurity and cyber resilience (**Cybersecurity Documentation and Controls**) in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network (**Minimum Cybersecurity Requirements**).

Particulars

Details of the Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum Cybersecurity Requirements are provided in paragraphs 14 and 15 below and Schedule A.

RI Advice should have had those Cybersecurity Documentation and Controls in place by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above; and

(b) the obligations pleaded in paragraphs 11 and 12 above,

and at trial ASIC will rely on the expert report of Shane Bell dated 30 April 2021 (**Bell Report**) in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

14 Further to paragraph 13 above, at all material times, the Cybersecurity Documentation and Controls that RI Advice should have had in place in order to

meet the Minimum Cybersecurity Requirements should have adequately addressed each of the following 13 cybersecurity domains:

1) Governance and business environment;

2) Risk assessments and risk management;

3) Asset management;

4) Supply chain risk management;

5) Access management;

6) Personnel security, training and awareness;

7) Data security;

8) Secure system development life cycle and change management;

9) Baseline operational security;

10) Security continuous monitoring;

11) Vulnerability management;

12) Incident response and communications; and

13) Continuity and recovery planning,

(**13 Cybersecurity Domains**).

Particulars

Details of the Cybersecurity Documentation and Controls that RI Advice should have had in place for each of the 13 Cybersecurity Domains in order to meet the Minimum Cybersecurity Requirements are provided in Schedule A.

Cybersecurity domains refer to subset areas of a cybersecurity framework which contain further granular cybersecurity controls. Examples of cybersecurity domains include ‘Access management’ and ‘risk assessments and risk management’.

A cybersecurity framework is a defined structure specific to cybersecurity which will generally comprise the mandated rules and processes to help an organisation reduce its cybersecurity risk to an acceptable level.

RI Advice was required to have Cybersecurity Documentation and Controls in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network. The obligation was upon RI Advice.

The Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum Cybersecurity Requirements should have adequately addressed each of the 13 Cybersecurity Domains by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

RI Advice should have had each of the Cybersecurity Documentation and Controls specified in Schedule A in place in each of the 13 Cybersecurity Domains at all material times in order to meet the Minimum Cybersecurity Requirements by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

15 Further to paragraphs 13 and 14 above, at all material times, as part of the Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum Cybersecurity Requirements, and in respect of its responses to cybersecurity incidents that occurred at RI Advice or within its AR network (**Cybersecurity Incidents**), RI Advice should have:

(a) identified the root cause of each Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of each Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from each Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network of gaps or deficiencies in the relevant Cybersecurity Documentation and Controls;

(ii) seeking technical security assurance across a number of its ARs, as a technical measure of the cybersecurity risks that exist in their organisations (**Technical Security Assurance**);

Particulars

RI Advice should have obtained Technical Security Assurance across a number of its ARs from an information technology specialist by using a methodology of the following nature:
(a) performing a technical controls review of the ARs' desktop computers, servers, network infrastructure and cloud-based environment, and reporting at a technical level of detail;
(b) performing a vulnerability assessment across its entire population of ARs identifying, quantifying, and prioritising

vulnerabilities identified in the ARs' information assets or systems; or (c) performing penetration testing of a targeted handful of ARs in order to understand whether they are susceptible to the same compromises that were the subject of each Cybersecurity Incident.

(iii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iv) developing and implementing a cybersecurity remediation plan for each Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in the relevant Cybersecurity Documentation and Controls.

Particulars

In respect of the Cybersecurity Incidents, RI Advice should have taken the steps pleaded in paragraphs 15(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraphs 13 and 14 above,

and at trial ASIC will rely on the Bell Report in relation to the appropriate responses to Cybersecurity Incidents.

C. CYBERSECURITY INCIDENTS BETWEEN 2014 AND MAY 2018

16 At all material times since about 2014;

(a) RI Advice has recorded details regarding the identification, management and close out of incidents concerning itself and its ARs, including Cybersecurity Incidents, in one or more Aligned Dealer Groups incident register databases (**Aligned Dealer Group Incident Register**), which:

(i) until about 30 September 2018, was maintained with the assistance of ANZ; and

(ii) since about 1 October 2018, has been maintained with the assistance of IOOF;

(b) alternatively, until about 30 September 2018, ANZ, and since about 1 October 2018, IOOF, has recorded details regarding the identification, management and close out of incidents concerning RI Advice and its ARs, including Cybersecurity Incidents, in the Aligned Dealer Group Incident Register, and RI Advice was aware of, or ought to have been aware of, the information concerning itself and its ARs in the Aligned Dealer Group Incident Register.

Particulars

In respect of sub-paragraph (b) above, RI Advice was aware of the details and information concerning the identification, management and close out of incidents concerning its ARs, including Cybersecurity Incidents, in the Aligned Dealer Group Incident Register because until about 30 September 2018, ANZ acted as an agent of RI Advice, and since about 1 October 2018, IOOF acted as an agent of RI Advice, in maintaining, and recording Cybersecurity Incidents concerning RI Advice and its ARs in, the Aligned Dealer Group Incident Register; and RI Advice was able to view the information in the Aligned Dealer Group Incident Register pertaining to RI Advice and its ARs and could generate reports and spreadsheets from the Aligned Dealer Group Incident Register and therefore was aware of, or ought to have been aware of, the details and information concerning the identification, management and close out of incidents concerning RI Advice and its ARs, including Cybersecurity Incidents, in the Aligned Dealer Group Incident Register.

In respect of sub-paragraphs (a) and (b) above, the documents below are examples of such reports and spreadsheets that could be

generated from the Aligned Dealer Group Incident Register by RI Advice.

A register titled 'ADG Incident register_Incident Data Report – All time.xlsx' (**ADG Incident Register Incident Data Report**) containing a total of 706 incidents relating to RI Advice and its ARs which are all denoted by an 'INC' identifier [FFG.1016.0001.0004], which was produced to ASIC by RI Advice in response to a notice S01973595 dated 21 March 2019.

A register titled 'COR reporting system_ADG Case Records (d1.01) 181005b.xlsx' (**COR Reporting System ADG Case Records**) containing a total of 156 reportable events relating to RI Advice and its ARs which are all denoted by a 'RE' identifier [FFG.1016.0001.0005], which was produced to ASIC by RI Advice in response to a notice S01973595 dated 21 March 2019.

A register titled 'IOOF COR Incident Master Spreadsheet_20181001_IOOF_COR Incident Master Spreadsheet.xlsx' (**IOOF COR Incident Master Spreadsheet**) containing a total of 42 IOOF COR incidents relating to RI Advice and its ARs which are all denoted by a 'IFR' identifier, and a total of 182 pre-IOOF COR incidents attributable to RI Advice with various forms of denotation [FFG.1016.0001.1389], which was produced to ASIC by RI Advice in response to a notice S01973595 dated 21 March 2019.

A register titled '20190521 - RI Incident Data Report' (**RI Incident Data Report**) containing a total of 147 incidents attributable to RI Advice and its ARs which are all denoted by an 'INC' identifier [RIF.0003.0103.0524], which was produced to ASIC by RI Advice in response to a notice S02513636 dated 18 November 2019.

C.1 Lifewise Cybersecurity Incident – July 2014

17 At all material times since about 17 August 2013, Lifewise Financial Solutions Pty Ltd until about 3 October 2017 as trustee for the Hickman-Bell Trust, and

thereafter as trustee of the Lifewise Financial Solutions Trust (**Lifewise**) was and is:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee;

(c) trading as Lifewise Financial Solutions; and

(d) engaged in providing financial services, on RI Advice's behalf, to Retail Clients.

18 At all material times, Bradley Ewan Rogers (**Rogers**) was and is:

(a) since about 17 August 2013:

(i) an AR of RI Advice;

(ii) not an AR of any other financial services licensee;

(iii) engaged in providing financial services, on RI Advice's behalf, to Retail Clients; and

(iv) until about 24 October 2016, an employee of Lifewise Financial Solutions Pty Ltd;

(b) since about 24 October 2016, a principal of Lifewise and the sole director of Lifewise Financial Solutions Pty Ltd.

19 On or about 7 or 9 July 2014, RI Advice became aware, or ought to have become aware, of a Cybersecurity Incident involving Rogers and Lifewise that had occurred in about early July 2014 (**Lifewise Cybersecurity Incident**).

Particulars

The Lifewise Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with 'logged', 'submitted' and 'report sent' dates of 7 July 2014 and an incident number of INC-194437 [FFG.1016.0001.0004] and in the Tab 'Pre-IOOF COR

Incident Register' of the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389].

The IOOF COR Incident Master Spreadsheet in the Tab 'Pre-IOOF COR Incident Register' (row 13 column P) records that Peter Ornsby, the CEO of RI Advice, was informed of the incident on or about 9 July 2014.

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

20 By about 5 November 2014 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the Lifewise Cybersecurity Incident, that it had been reported that:

(i) an unknown third party had hacked Rogers' Google email account;

(ii) five Lifewise Retail Clients had been sent a malicious email which appeared to have been sent from Rogers' Google email account (**Malicious Lifewise Emails**);

(iii) the Malicious Lifewise Emails requested the five Lifewise Retail Clients to transfer funds to an unknown external party;

(iv) on about 5 July 2014, one Lifewise Retail Client, who had been sent one of the Malicious Lifewise Emails (**Lifewise Cyber Fraud Victim**), transferred $60,000 to an unknown external party bank account; and

(v) the Lifewise Cyber Fraud Victim had not as yet recovered $35,000 of the $60,000 that she had transferred; and

(b) had endorsed or allowed the Lifewise Cybersecurity Incident to be recorded and closed out in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by Lifewise and RI Advice

in respect of the Lifewise Cybersecurity Incident, prior to the incident being closed out in the Aligned Dealer Group Incident Register, were limited to the following:

(i) Rogers had changed his email address and communicated this to clients;

(ii) Lifewise had notified clients that they should notify Rogers if they received any other suspicious emails;

(iii) the police had been notified;

(iv) Lifewise confirmed that no other clients of Lifewise had transferred money;

(v) ANZ Group Investigations had prepared an investigation report; and

(vi) the Lifewise Cyber Fraud Victim was working with police and her financial institution to attempt to recover the remaining defrauded monies.

Particulars

The various reported matters and steps taken in respect of the Lifewise Cybersecurity Incident referred to in sub-paragraphs (a) to (c) above were recorded in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389] and the Lifewise Cybersecurity Incident was recorded as closed as at 5 November 2014 in the ADG Incident Register Incident Data Report [FFG.1016.0001.0004].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

21 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15 and 17 to 20 above, after becoming aware, or after it ought to have become aware, of the Lifewise Cybersecurity Incident and prior to endorsing or allowing the closure of the Lifewise Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified the root cause of the Lifewise Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the Lifewise Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from the Lifewise Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the Lifewise Cybersecurity Incident:

(A) Cyber training and awareness;

(B) Multi-factor authentication;

(C) Incident response; and

(D) Email filtering; and

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Cyber training and awareness [ED 6.1 to ED 6.7];

(b) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(c) Incident response [ED 12.1 to ED 12.5]; and

(d) Email filtering [ED 9.4 and ED 9.8].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the Lifewise Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the Lifewise Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 21(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 17 to 20 above,

and at trial ASIC will rely on the Bell Report.

22 RI Advice did not take the steps referred to in paragraph 21 above, adequately or at all, by 15 May 2018 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 20(c) above, which did not amount to taking the steps referred to in paragraph 21 above adequately or at all.

C.2 RI Advice Corporate Cybersecurity Incident – May 2015

23 On or about 8 May 2015, RI Advice became aware, or ought to have become aware, that it was possible for any person to access internal corporate RI Advice documents located on RI Advice's internal intranet site (**RI Intranet**) via the Internet (**RI Corporate Cybersecurity Incident**).

Particulars

The RI Corporate Cybersecurity Incident was recorded in the Tab 'Pre-IOOF COR Incident Register' of the IOOF COR Incident Master Spreadsheet with 'COR Date Entered', 'submitted' and 'report sent' dates of 8 May 2015 (incident reference LE_1117650) [FFG.1016.0001.1389].

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

24 By about 22 December 2016 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the RI Corporate Cybersecurity Incident, that it had been reported that:

(i) the RI Corporate Cybersecurity Incident had occurred since about 2012;

(ii) the RI Intranet contained commercially sensitive RI Advice documents including relating to communications, templates and processes; and

(iii) the documents located on the RI Intranet were publicly accessible and searchable including through the use of a Google search without the requirement for any password;

(b) had endorsed or allowed the RI Corporate Cybersecurity Incident to be recorded and closed out in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by RI Advice in respect of the RI Corporate Cybersecurity Incident, prior to the incident being closed out in the Aligned Dealer Group Incident Register, were limited to the following:

(i) in about May 2015, RI Advice contacted an external organisation which was asked to investigate and rectify the incident;

(ii) in about early 2016, RI Advice commenced a plan to transition the RI Intranet to a new Intranet provider using a new secure site;

(iii) since about September or October 2016, RI Advice engaged external parties to perform IT and security tests on the new secure site;

(iv) since about 3 November 2016, RI Advice transitioned the RI Intranet to the new secure site; and

(v) on or about 18 November 2016, RI Advice received a final security test report in respect of the new secure site.

Particulars

The various reported matters and steps taken in respect of the RI Corporate Cybersecurity Incident referred to in sub-paragraphs (a) to (c) above were recorded in the Tab 'Pre-IOOF COR Incident Register' of the IOOF COR Incident Master Spreadsheet (incident reference LE_1117650) [FFG.1016.0001.1389].

The IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389] recorded that between about 1 May and 2 June 2015, RI Advice, through Jason Gapps in Marketing, had requested and followed up with FuseFarm to investigate and rectify the RI Corporate Cybersecurity Incident.

The IOOF COR Incident Master Spreadsheet recorded that the RI Advice Event Working Group reported on 6 October 2016 that RI Advice had engaged Felix Alvarez for the security review and EY for the penetration test of the new secure site.

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

25 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15, 23 and 24 above, after becoming aware, or after it ought to have become aware, of

the RI Corporate Cybersecurity Incident and prior to endorsing or allowing the closure of the RI Corporate Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified the root cause of the RI Corporate Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the RI Corporate Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from the RI Corporate Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the RI Corporate Cybersecurity Incident:

(A) Multi-factor authentication;

(B) Incident response; and

(C) Technical security testing; and

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(b) Incident response [ED 12.1 to ED 12.5]; and

(c) Technical security testing [ED 11.3].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the RI Corporate Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the RI Corporate Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 25(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 23 to 24 above,

and at trial ASIC will rely on the Bell Report.

26 RI Advice did not take the steps referred to in paragraph 25 above, adequately or at all, by 15 May 2018 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 24(c) above, which did not amount to taking the steps referred to in paragraph 25 above adequately or at all.

C.3 Firefly Cybersecurity Incident – June 2015

27 At all material times from about 12 August 2013 to about 9 May 2016, and since about 9 January 2017, the Trustee for the Griffin Martin Investment Trust trading as Firefly Wealth (**Firefly Wealth**) was and is:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee;

(c) trading as Firefly Wealth; and

(d) engaged in providing financial services, on RI Advice's behalf, to Retail Clients.

28 At all material times from about 8 December 2012 to about 9 May 2016 and since about 9 January 2017, Adele Martin (**Martin**) was and is:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee;

(c) engaged in providing financial services, on RI Advice's behalf, to Retail Clients; and

(d) the organisational representative of Firefly Wealth.

29 On or about 17 June 2015, RI Advice became aware, or ought to have become aware, of a Cybersecurity Incident involving Martin and Firefly Wealth that had occurred in June 2015 (**Firefly Cybersecurity Incident**).

Particulars

The Firefly Cybersecurity Incident was recorded in the IOOF COR Incident Master Spreadsheet (incident reference 4593) with a 'COR date entered' of 17 June 2015 [FFG.1016.0001.1389].

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

30 By about 22 June 2015 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the Firefly Cybersecurity Incident, that it had been reported that:

(i) the website belonging to Innergi, a third party organisation responsible for website and email newsletter content provided to Firefly's Retail Clients and advisers, was hacked between about 16 and 17 June 2015 and defaced by a threat actor purporting to be ISIS; and

(ii) hackers had put a fake home page on top of the knowledge centre website which meant that Retail Clients accessing the home page could not get through to the knowledge centre on the website;

(b) had endorsed and allowed the Firefly Cybersecurity Incident to be recorded and closed out in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by Firefly and RI Advice in respect of the Firefly Cybersecurity Incident, prior to the incident being closed out in the Aligned Dealer Group Incident Register, were limited to the following:

(i) Innergi had confirmed that the website did not hold client data and it had been removed while they investigated the matter; its website was held on a separate server domain to the client data; and its other computer server which held client data including names and email addresses had not been hacked;

(ii) Innergi had confirmed that it had uploaded additional security software and, after testing, had confirmed that it had no malware, spam or suspicious code, and the website had no vulnerabilities and was fully functional by midday on 17 June 2015;

(iii) Innergi confirmed it was being acquired by IRESS and it was in the process of moving to IRESS's servers in due course; and

(iv) ANZ IT security had been notified of the incident.

Particulars

The various reported matters and steps taken in respect of the Firefly Cybersecurity Incident referred to in sub-paragraphs (a) to (c) above were recorded in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

31 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15 and 27 to 30 above, after becoming aware, or after it ought to have become aware, of the Firefly Cybersecurity Incident and prior to endorsing or allowing the closure of the Firefly Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified the root cause of the Firefly Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the Firefly Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from the Firefly Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the Cybersecurity Documentation and Controls relevant to the Firefly Cybersecurity Incident, comprising Third party risk management controls;

Particulars

Details of the Third party risk management controls [ED 4.1 to ED 4.3] are provided in Schedule A.

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the Firefly Cybersecurity Incident which was tailored to the identified

cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the Firefly Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 31(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 27 to 30 above,

and at trial ASIC will rely on the Bell Report.

32 RI Advice did not take the steps referred to in paragraph 31 above, adequately or at all, by 15 May 2018 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 30(c) above, which did not amount to taking the steps referred to in paragraph 31 above adequately or at all.

C.4 JEM Wealth Cybersecurity Incident – September 2016

33 At all material times from about 17 October 2014 until about 3 May 2018, Benjamin McHugh (**McHugh**) was:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee;

(c) engaged in providing financial services, on RI Advice's behalf, to Retail Clients; and

(d) a principal of a financial advice business trading as JEM Wealth (**JEM Wealth**).

34 On or about 6 September 2016, RI Advice became aware, or ought to have become aware, of a Cybersecurity Incident involving McHugh (**JEM Wealth Cybersecurity Incident**).

Particulars

The JEM Wealth Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with a 'COR date entered' of 6 September 2016 and incident number INC-373428 [FFG.1016.0001.0004] and in the Tab 'Pre-IOOF COR Incident Register' of the IOOF COR Incident Master Spreadsheet with incident reference RE_018405 [FFG.1016.0001.1389].

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

35 By about 31 October 2016 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the JEM Wealth Cybersecurity Incident, that it had been reported that:

(i) a JEM Wealth Retail Client had informed JEM Wealth that she had been sent a suspicious email that requested money and which appeared to have been sent from McHugh's email account (**Malicious McHugh Email**);

(ii) McHugh did not send the Malicious McHugh Email; and

(iii) JEM Wealth used 'Microsoft Outlook 360' and all of its information was stored 'in the Cloud'; it had no anti-virus software installed on its systems; and there was one password which everyone in the practice used to access the information stored 'in the Cloud';

(b) had endorsed or allowed the JEM Wealth Cybersecurity Incident to be recorded and closed out in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by JEM Wealth and RI Advice in respect of the JEM Wealth Cybersecurity Incident, prior to the incident being closed out in the Aligned Dealer Group Incident Register, were limited to the following:

(i) ANZ Legal & Group Investigations had been notified of the incident, and they advised that JEM Wealth should arrange for an information technology person to check out their systems;

(ii) relevant financial product providers were to be contacted to flag all transactions associated with McHugh's advisor code and JEM Wealth was requested to ensure that its data was securely backed up;

(iii) JEM Wealth confirmed that it had installed anti-virus software and that it had changed the password to access documents stored in the Cloud;

(iv) all JEM Wealth staff continued to have access to the same password;

(v) JEM Wealth had notified clients of the incident and it had received no other inquiries from clients in response to the incident; and

(vi) no further 'targeted review' was required.

Particulars

The various reported matters and steps taken in respect of the JEM Wealth Cybersecurity Incident referred to in sub-paragraphs (a) to (c) above were recorded in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389] and the JEM Wealth Cybersecurity Incident was recorded as closed as at 31 October 2016 in the ADG Incident Register Incident Data Report [FFG.1016.0001.0004].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

36 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15 and 33 to 35 above, after becoming aware, or after it ought to have become aware, of the JEM Wealth Cybersecurity Incident and prior to endorsing or allowing the closure of the JEM Wealth Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified the root cause of the JEM Wealth Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the JEM Wealth Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from the JEM Wealth Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the JEM Wealth Cybersecurity Incident:

(A) Cyber training and awareness;

(B) Multi-factor authentication;

(C) Incident response; and

(D) Email filtering; and

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Cyber training and awareness [ED 6.1 to ED 6.7];

(b) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(c) Incident response [ED 12.1 to ED 12.5]; and

(d) Email filtering [ED 9.4 and ED 9.8].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the JEM Wealth Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the JEM Wealth Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 36(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 33 to 35 above,

and at trial ASIC will rely on the Bell Report.

37 RI Advice did not take the steps referred to in paragraph 36 above, adequately or at all, by 15 May 2018 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 35(c) above, which did not amount to taking the steps referred to in paragraph 36 above adequately or at all.

C.5 Wise Cybersecurity Incident – December 2016

38 At all material times until about 16 January 2019, Anthony Hilsley (**Hilsley**) was:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee;

(c) engaged in providing financial services, on RI Advice's behalf, to Retail Clients; and

(d) a principal and director of Superannuation Advisory Service Pty Ltd trading as Wise Financial Planning and/or SAS Advice (**Wise Financial Planning**).

39 On or about 3 January 2017, RI Advice became aware, or ought to have become aware, of a Cybersecurity Incident involving Hilsley and Wise Financial Planning (**Wise Cybersecurity Incident**).

Particulars

The Wise Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with 'logged', 'submitted' and 'report sent' dates of 3 January 2017 and an incident number of INC-336398 [FFG.1016.0001.0004] and in the Tab 'Pre-IOOF COR Incident Register' of the IOOF COR Incident Master Spreadsheet with an incident reference of RE_022633 [FFG.1016.0001.1389].

Letter from RI Advice to ASIC dated 25 January 2019 in response to Notice issued by ASIC under s 912C of ASIC Act [FFG.1013.0001.0003 at 0005].

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

40 By about 20 February 2017 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the Wise Cybersecurity Incident, that it had been reported that:

(i) from about 26 December 2016 to about 1 January 2017, Wise Financial Planning's main reception computer was hacked by ransomware software delivered by email; and

(ii) as a consequence, a number of Wise Financial Planning's electronic files were encrypted and made inaccessible;

(b) had endorsed or allowed the Wise Cybersecurity Incident to be recorded and closed out in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by Wise Financial Planning and RI Advice in respect of the Wise Cybersecurity Incident, prior to the incident being closed out in the Aligned Dealer Group Incident register, were limited to the following:

(i) Wise Financial Planning had notified police, who had confirmed that the issue was becoming very common, lodged the matter with the Australian Cybercrime Online Reporting Network (**ACORN**), contacted relevant financial product providers and requested a 'flag' on client records;

(ii) Wise Financial Planning's external IT provider had reviewed affected server files, and had done a 'clean' of the server, placed additional unspecified 'security measures' on Wise Financial Planning's server, 'updated' passwords on unspecified devices and ensured by unspecified means that there were 'no back door security gaps', and confirmed that client data had not been affected by the incident; and

(iii) the RI Advice Event Working Group had endorsed that no 'targeted review' was required.

Particulars

The various reported matters and steps taken in respect of the Wise Cybersecurity Incident referred to in sub-paragraphs (a) to (c) above were recorded in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389] and the Wise Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with a close out date of 20 February 2017 [FFG.1016.0001.0004].

Letter from RI Advice to ASIC dated 25 January 2019 in response to Notice issued by ASIC under s 912C of ASIC Act [FFG.1013.0001.0003 at 0005].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

41 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15 and 38 to 40 above, after becoming aware, or after it ought to have become aware, of the Wise Cybersecurity Incident and prior to endorsing or allowing the closure of the Wise Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the Wise Cybersecurity Incident referred to in paragraph 40(a)(i) above; and

(b) incorporated the findings about the root cause and lessons learnt from the Wise Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security

Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the Wise Cybersecurity Incident:

(A) Cyber training and awareness;

(B) Email filtering;

(C) Application whitelisting;

(D) Privilege management; and

(E) Incident response; and

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Cyber training and awareness [ED 6.1 to ED 6.7];

(b) Email filtering [ED 9.4 and ED 9.8];

(c) Application whitelisting [ED 9.2 and ED 9.5];

(d) Privilege management [ED 5.3, ED 5.5 and ED 10.6]; and

(e) Incident response [ED 12.1 to ED 12.5]; and

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the Wise Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the Wise Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 41(a) and (b) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 38 to 40 above,

and at trial ASIC will rely on the Bell Report.

42 RI Advice did not take the steps referred to in paragraph 41 above, adequately or at all, by 15 May 2018 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 40(c) above, which did not amount to taking the steps referred to in paragraph 41 above adequately or at all.

C.6 RI Circular Quay Cybersecurity Incident – May 2017

43 At all material times, John Leslie Walker (**Walker**) was and is:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee;

(c) engaged in providing financial services, on RI Advice's behalf, to Retail Clients; and

(d) a principal of a financial advice business trading as RetireInvest Circular Quay (**RI Circular Quay**).

44 On or about 30 May 2017, RI Advice became aware, or ought to have become aware, of a Cybersecurity Incident involving RI Circular Quay that had occurred over the course of the past day (**RI Circular Quay Cybersecurity Incident**).

Particulars

Email from Janelle Carey of RI Circular Quay to Advice Risk, copied to Joseph Ayrout, RI Advice, dated 30 May 2017 re RI Circular Quay - Desktop PC hacked [RIF.0004.0004.7817].

Tab 'Pre-IOOF COR Incident Register' in the IOOF COR Incident Master Spreadsheet with an incident reference of RE_028669 and 'Date Discovered' date of 30 May 2017 and 'COR Entered' date of 6 June 2017 [FFG.1016.0001.1389].

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

45 Between about 30 May and 3 October 2017, RI Advice:

(a) became aware, or ought to have become aware, that RI Circular Quay had reported in respect of the RI Circular Quay Cybersecurity Incident that:

(i) a computer server on RI Circular Quay's local computer network had been hacked by brute force through a remote access port;

(ii) RI Circular Quay's shared office files had been encrypted and as a result RI Circular Quay staff were not able to access them;

(iii) RI Circular Quay had been asked to pay a ransom to have the files unencrypted and made accessible;

(iv) RI Circular Quay did not have a backup system in place;

(v) unless RI Circular Quay paid a ransom the encrypted data was not recoverable;

(vi) the encrypted data included statement of advice records (which contained customers' names, addresses, dates of birth and financial records), Centrelink customer numbers, fund manager

names and policy numbers, bank account details and tax file numbers; and

(vii) approximately 226 client files had been affected;

Particulars

Email from Janelle Carey of RI Circular Quay to Advice Risk, copied to Joseph Ayrout, RI Advice dated 30 May 2017 re RI Circular Quay - Desktop PC hacked [RIF.0004.0004.7817].

Email from Janelle Carey of RI Circular Quay to Advice Risk dated 6 June 2017 re RI Circular Quay - Desktop PC hacked [RIF.0004.0004.4704].

Email from Janelle Carey of RI Circular Quay to Advice Risk dated 9 June 2017 re RI Circular Quay - Desktop PC hacked Acorn Reference No. ARN-PC64-TRK4 [RIF.0004.0004.4704].

Email from Advice Risk to Janelle Carey of RI Circular Quay, copied to Joseph Ayrout, RI Advice, dated 23 June 2017 attaching spreadsheet entitled 'List of Clients Affected with date of birth' [RIF.0004.0004.4716 and RIF.0004.0004.4723].

Email from Janelle Carey of RI Circular Quay to Advice Risk, copied to Joseph Ayrout, RI Advice, dated 26 June 2017 re RI Circular Quay - Desktop PC hacked Acorn Reference No. ARN-PC64-TRK4 [RIF.0004.0004.4704].

Email from Janelle Carey of RI Circular Quay to Advice Risk, copied to Joseph Ayrout, RI Advice, dated 17 July 2017 attaching spreadsheet entitled 'List of Clients Affected with date of birth' [RIF.0004.0004.4704 and RIF.0004.0004.4715].

Email from Joncarl La Rosa of RI Circular Quay to George Reinoso, Nicholas Ponniah and Joseph Ayrout, RI Advice, dated 9 August 2017 re RI ACORN Report submission ARN-PC64-TRK4 [RIF.0004.0004.6929].

The RI Circular Quay Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report [FFG.1016.0001.0004] and in the Tab 'Pre-IOOF COR Incident Register' in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389].

(b) had not obtained sufficiently detailed information from RI Circular Quay in order to determine the root cause of the RI Circular Quay Cybersecurity Incident; and

Particulars

Email from Joncarl La Rosa of RI Circular Quay to George Reinoso, Nicholas Ponniah and Joseph Ayrout, RI Advice, dated 9 August 2017 re RI ACORN Report submission ARN-PC64-TRK4 [RIF.0004.0004.6929].

(c) endorsed or allowed the RI Circular Quay Cybersecurity Incident to be retained in the Aligned Dealer Group Incident Register as an 'open' incident, or ought to have become aware that this had occurred.

Particulars

As referred to in paragraph 47 below, the RI Circular Quay Cybersecurity Incident was not closed out until about 3 October 2018 and was open for approximately 484 days before being closed out.

The RI Circular Quay Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with 'logged', 'submitted' and 'report sent' dates of 6 June 2017 and a 'close' date of 3 October 2018 (incident number INC-115056) [FFG.1016.0001.0004] and a 'COR date entered' of 6 June 2017 in the Tab 'Pre-IOOF COR Incident Register' in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

46 By about 4 October 2017, RI Advice was aware that:

(a) RI Advice was only able to provide very minimal support to RI Circular Quay to seek to ensure that that such a Cybersecurity Incident did not happen again as RI Advice did not have any specific cybersecurity specifications or guidelines; and

(b) ANZ's Manager of Security and Technology Risk Services had recommended to RI Advice that RI Advice ask ANZ's Cyber Security Operations team to conduct an assessment of the technical environments of the various RI Advice AR offices.

Particulars

Email exchange involving Joseph Ayrout, Practice Development Leader, RI Advice, Peter Ornsby, CEO of RI Advice and Tessa Micock, ANZ, and David Perger, ANZ dated 3 and 4 October 2017 RE: Privacy Consideration: RI Circular Quay [RIF.0004.0004.4665].

47 The RI Circular Quay Cybersecurity Incident recorded in the Aligned Dealer Incident Register:

(a) remained open as at 15 May 2018;

(b) was not closed out until about 3 October 2018; and

(c) was open for approximately 484 days before being closed out.

Particulars

The RI Circular Quay Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with a 'close' date of 3 October 2018 [FFG.1016.0001.0004].

48 As at 15 May 2018, RI Advice had recorded, or ANZ had recorded as agent of RI Advice, that the remediation and follow up steps undertaken by RI Circular Quay and RI Advice in respect of the RI Circular Quay Cybersecurity Incident were limited to the following:

(a) the incident had been reported to ACORN;

(b) RI Circular Quay had reported that the desktop computer was completely reset and all software reloaded; anti-virus software had been loaded on all computer systems; remote access had been disabled and all staff had been requested to change their email passwords; and the office internet router password had been changed;

(c) relevant financial product providers had been contacted, and a caution flag had been placed on the customers' accounts to mitigate potential fraud attempts;

(d) ANZ had been provided with a list of affected RI Circular Quay clients so that additional security could be placed on the accounts; and

(e) RI Circular Quay had notified approximately 222 impacted clients and recommended that they update passwords and contact http://www.idcare.org/ for further support.

Particulars

Email from Janelle Carey of RI Circular Quay to Advice Risk dated 6 June 2017 re RI Circular Quay - Desktop PC hacked [RIF.0004.0004.4704].

Email from Janelle Carey of RI Circular Quay to Advice Risk dated 9 June 2017 re RI Circular Quay - Desktop PC hacked Acorn Reference No. ARN-PC64-TRK4 [RIF.0004.0004. 4704].

Email from Janelle Carey of RI Circular Quay to Advice Risk, copied to Joseph Ayrout, RI Advice, dated 26 June 2017 re RI Circular Quay - Desktop PC hacked Acorn Reference No. ARN-PC64-TRK4 [RIF.0004.0004. 4704].

Email from Janelle Carey of RI Circular Quay to Advice Risk, copied to Joseph Ayrout, RI Advice, dated 17 July 2017 attaching spreadsheet entitled 'List of Clients Affected with date of birth' [RIF.0004.0004.4704 and RIF.0004.0004.4715].

Email from Advice Risk to Tessa Micock and Joncarl La Rosa, copied to Peter Ornsby, RI Advice, dated 3 October 2017 Re Privacy Considerations [RIF.0004.0004.4695].

The RI Circular Quay Cybersecurity Incident was recorded in the ADG Incident Register Incident Data Report with 'logged', 'submitted' and 'report sent' dates of 6 June 2017 [FFG.1016.0001.0004] and a 'COR Date Entered' of 6 June 2017 in the Tab 'Pre-IOOF COR Incident Register' in the IOOF COR Incident Master Spreadsheet [FFG.1016.0001.1389].

Letter from RI Advice to ASIC dated 25 January 2019 in response to Notice issued by ASIC under s 912C of ASIC Act [FFG.1013.0001.0003 at 0005].

Further, as to ANZ acting as agent of RI Advice, the plaintiff refers to and repeats paragraph 16 above.

49 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 and 15 and 43 to 48 above, after becoming aware, or after it ought to have become aware, of the RI Circular Quay Cybersecurity Incident, RI Advice should have:

(a) identified the root cause of the RI Circular Quay Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the RI Circular Quay Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from the RI Circular Quay Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking technical security assurance across a number of its ARS, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the RI Circular Quay Cybersecurity Incident:

(A) Account lockout policies;

(B) Password complexity;

(C) Multi-factor authentication;

(D) Port security;

(E) Log monitoring;

(F) Incident response;

(G) Patch management; and

(H) Backups; and

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Account lockout policies [ED 5.3];

(b) Password complexity [ED 5.1 and ED 7.1];

(c) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(d) Port security [ED 9.4 and ED 9.8];

(e) Log monitoring [ED 10.1 to ED 10.6];

(f) Incident response [ED 12.1 to ED 12.5];

(g) Patch management [ED 11.2 and ED 11.4]; and

(h) Backups [ED 13.3 and ED 13.5].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the RI Circular Quay Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network,

including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the RI Circular Quay Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 49(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 43 to 48 above,

and at trial ASIC will rely on the Bell Report.

50 RI Advice did not take the steps referred to in paragraphs 46(b) and 49 above, adequately or at all, by 15 May 2018 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 48 above, which did not amount to taking the steps referred to in paragraphs 46(b) and 49 above adequately or at all.

C.7 FFG Data Breach – December 2017 to April 2018

51 At all material times, Frontier Financial Group Pty Ltd as trustee for The Frontier Trust (**FFG**) was and is:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee; and

(c) engaged in providing financial services, on RI Advice's behalf, to Retail Clients.

52 From about 30 December 2017 until about 15 April 2018, an unknown malicious agent obtained and retained unauthorised remote access to FFG's file server (**FFG Data Breach**), through an FFG employee's account.

53 During the FFG Data Breach, the malicious agent spent a total of more than 155 hours logged into the FFG file server.

54 The compromised FFG file server contained Personal Information including documents recording client names, addresses, tax file numbers, transaction account numbers, transaction details, identification documents, and, in some cases, health information.

Particulars

The data contained on the compromised FFG file server is referred to the 'Event Closure Report – RI Advice: Frontier Financial Group (FFG) Notifiable Data Breach (NBD) – FINAL' dated 18 September 2019 – [FFG.1020.0001.0154] and in the KPMG Retire Invest Pty Ltd Cyber Incident Response – Forensic Review dated 24 October 2018 [PP2.1003.0002.0004].

55 FFG did not detect the FFG Data Breach until about 16 April 2018.

56 On or about 15 May 2018, RI Advice became aware:

(a) of the FFG Data Breach;

(b) that FFG had detected the FFG Data Breach on or about 16 April 2018; and

(c) that three FFG Retail 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 that had been opened, without their consent.

Particulars

Telephone call between Richard McLean, the proprietor of FFG, and Peter Ornsby, CEO of RI Advice, referred to in email between

Peter Ornsby and Advice Risk dated 15 May 2018 Re Frontier Financial [FFG.0014.0001.0179].

The FFG Data Breach was recorded in the FFG ADG Incident Register Incident Data Report (incident review number IFR-01589) with 'discovery', 'logged', 'submitted' and 'report sent' dates of 15 May 2018 [FFG.1016.0001.0004].

Email from Steven Woodford of FFG to Peter Ornsby dated 15 May 2018 [FFG.0014.0001.0180].

Letter from RI Advice to ASIC dated 25 January 2019 in response to Notice issued by ASIC under s 912C of ASIC Act [FFG.1013.0001.0003 at 0006].

D. INADEQUACY OF STEPS TAKEN BY RI ADVICE UP TO 15 MAY 2018 AND INADEQUACY OF CYBERSECURITY SYSTEMS IN PLACE AS AT 15 MAY 2018

D.1 Inadequacy of May 2018 Cybersecurity Documentation and Controls

57 Prior to and as at 15 May 2018, the Cybersecurity Documentation and Controls that RI Advice held or had access to for the management of risk in respect of cybersecurity and cyber resilience across its AR network were as follows:

(a) ANZ Aligned Licensees & Advice Standards, Business Continuity, version 1.0, date of rehearsal 19 March 2018 [FFG.1022.0001.1916];

(b) ANZ Aligned Licensees & Advice Standards, Governance Framework, version 2.0, dated April 2017 [FFG.1012.0001.0197];

(c) ANZ Business Continuity and Crisis Management Policy, version 5, dated April 2018 [FFG.1022.0001.0559];

(d) ANZ Business Continuity Management, Enablement & Governance dated September 2016 [FFG.1022.0001.0570];

(e) ANZ Control 37 - Disaster Recovery Tests have been prepared and are tested on a regular basis [FFG.1022.0001.0545];

(f) ANZ Disaster Recovery Issues Work Instructions dated about February 2014 [FFG.1022.0001.0598];

(g) Electronic Storage Guide, version 1.0, released 26 March 2018, effective 1 May 2018 [FFG.1002.0001.0005];

(h) ANZ Global Operational Risk Library, Risk Library Index, version 4.0, dated 15 August 2013 [FFG.1018.0001.0216];

(i) ANZ Information Security Standard, version 1.0, dated February 2016 [FFG.1022.0001.0747];

(j) ANZ Operational Risk – Change Management Process, version 2.1, dated 8 January 2016 [FFG.1018.0001.0416];

(k) ANZ Operational Risk Capital Measurement Methodology, version 1.2, dated 21 July 2015 [FFG.1018.0001.0318];

(l) ANZ Operational Risk – Key Control Effectiveness, version 2.0, dated 1 April 2017 [FFG.1018.0001.0230];

(m) ANZ Operational Risk – Risk and Control Assessment, version 1.8, dated 28 June 2016 [FFG.1018.0001.0512];

(n) ANZ Operational Risk Measurement and Management Policy, version 4.0, dated December 2016 [FFG.1018.0001.0498];

(o) Privacy Standard, version 2.0, dated February 2018 [FFG.1022.0001.1205];

(p) Cybersecurity awareness presentations and guides;

Particulars

RI Advice – Cyberfraud presentation dated November 2014 [FFG.1007.0001.0093].

Kaplan Professional Cyber resilience: good practice and guidance dated November 2016 [FFG.1003.0001.0098].

Reboot. Reset. Cybercrime in business – taking back control dated 1 August 2017 [FFG.1022.0001.2570].

(q) RI Advice procedures, application forms and checklists for recruitment, appointment and cancellation of ARs and RI Advice Practices; and

Particulars

ADG Recruitment Fact Find (Version 15) dated February 2018 [FFG.1022.0001.2377].

Goldseal Human Resources Guidance Handbook (version 12) dated about February 2018 Section 8.10 (Reference checks) [FFG.1022.0002.0010].

RI Advice Practice Development Manager Application Checklist dated about 14 February 2018 [FFG.1022.0001.1760].

RI Advice APPOINTMENT: Authorised Representative Appointment Checklist dated about 6 February 2016 [FFG.1022.0001.1654].

RI Advice Authorised Representative Application Form, Version 18, April 2018 [FFG.1022.0001.1679].

RI Advice Practice Application Form Version 14, May 2017 [FFG.1022.0001.1702].

RI Advice Reference Check Form dated about July 2016 [FFG.1022.0001.1650].

(r) RI Advice, Section 3 of RI Advice Professional Standards Manual, Procedures and Policies dated July 2017 [FFG.1022.0001.0448]; and

(s) Service Level Agreements between RI Advice and ANZ;

Particulars

Service Level Agreement – Version 1" between ANZ (designated as "Supplier") and RI Advice (designated as "Licensee") dated 8 August 2012 [FFG.1015.0004.0008];

Service Level Agreement – Version 2" between ANZ (designated as "Supplier") and RI Advice (designated as "Licensee") dated 2 December 2013 [FFG.1015.0004.0021];

Service Level Agreement – Version 3" between ANZ (designated as "Supplier") and RI Advice (designated as "Licensee") dated 19 December 2014 [FFG.1015.0004.0043];

Service Level Agreement – Version 4" between ANZ (designated as "Supplier") and RI Advice (designated as "Licensee") dated 1 March 2016 [FFG.1015.0004.0065];

Service Level Agreement – Version 5" between ANZ (designated as "Supplier") and RI Advice (designated as "Licensee") dated 1 January 2017 [FFG.1015.0004.0087]; and

Service Level Agreement – Version 6" between ANZ (designated as "Supplier") and RI Advice (designated as "Licensee") dated 17 January 2018 [FFG.1015.0004.0109].

(the **May 2018 Documentation and Controls**).

58 Prior to and as at 15 May 2018, RI Advice did not have in place any Cybersecurity Documentation and Controls for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 57 above.

59 By its May 2018 Documentation and Controls, RI Advice:

(a) did not adequately document the roles and responsibilities of RI Advice and its ARs as to the management of risk in respect of cybersecurity and cyber resilience across its AR network;

(b) predominantly relied upon ANZ-developed documents, which:

(i) were specific to the ANZ organisation and its IT environment;

(ii) were not tailored to RI Advice and its ARs' requirements for the management of risk in respect of cybersecurity and cyber resilience across its AR network; and

Particulars

With the exception of the documents referred to in paragraphs 57(g), (i), (o), (p), (q) and (r) above, each of the May 2018 Documentation and Controls had the characteristics referred to in sub-paragraphs (i) and (ii) above.

(iii) had not been implemented and operationalised by RI Advice as part of its governance and management of risk in respect of cybersecurity and cyber resilience across its AR network;

Particulars

With the exception of the documents referred to in paragraphs 57(g), (p), (q) and (r) above, each of the May 2018 Documentation and Controls had the characteristics referred to in sub-paragraph (iii) above.

(c) did not adopt and implement adequate Cybersecurity Documentation and Controls in each of the 13 Cybersecurity Domains;

(d) did not meet the Minimum Cybersecurity Requirements; and

(e) did not adequately manage risk in respect of cybersecurity and cyber resilience across its AR network.

Particulars

In respect of sub-paragraphs (a), (c), (d) and (e) above, the gaps between the May 2018 Documentation and Controls and the Cybersecurity Documentation and Controls which RI Advice should have had in place in each of the 13 Cybersecurity Domains in order to meet the Minimum Cybersecurity Requirements are set out in Schedule B.

RI Advice was required to have Cybersecurity Documentation and Controls in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network. The obligation was upon RI Advice.

The Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum Cybersecurity Requirements should have adequately addressed each of the 13 Cybersecurity Domains by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

RI Advice should have had each of the Cybersecurity Documentation and Controls specified in Schedules A and B in place in each of the 13 Cybersecurity Domains prior to and as at 15 May 2018 in order to meet the Minimum Cybersecurity Requirements by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 to 15 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

D.2 Contraventions in respect of conduct up to and as at 15 May 2018

60 By reason of the matters pleaded in paragraphs 2 to 5, 11 to 15, 21, 22, 25, 26, 31, 32, 36, 37, 41, 42, 49, 50 and 57 to 59 above, as at 15 May 2018, RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act as at 15 May 2018, by reason of:

(i) the conduct pleaded in paragraph 59 above, and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above;

(ii) the conduct pleaded in paragraph 22 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 17 to 21 above;

(iii) the conduct pleaded in paragraph 26 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 23 to 25 above;

(iv) the conduct pleaded in paragraph 32 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 27 to 31 above;

(v) the conduct pleaded in paragraph 37 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 33 to 36 above;

(vi) the conduct pleaded in paragraph 42 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 38 to 41 above; and/or

(vii) the conduct pleaded in paragraph 50 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 43 to 49 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, as at 15 May 2018, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that the public is entitled to expect, as at 15 May 2018, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly

comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act as at 15 May 2018, by reason of:

(i) the conduct referred to in paragraph 59 above and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above;

(ii) the conduct pleaded in paragraph 22 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 17 to 21 above;

(iii) the conduct pleaded in paragraph 26 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 23 to 25 above;

(iv) the conduct pleaded in paragraph 32 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 27 to 31 above;

(v) the conduct pleaded in paragraph 37 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 33 to 36 above;

(vi) the conduct pleaded in paragraph 42 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 38 to 41 above; and/or

(vii) the conduct pleaded in paragraph 50 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 43 to 49 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws are detailed in paragraphs 13 to 15 above, and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 60(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 60(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 60(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 60(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15

above, RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience as at 15 May 2018 comprised the May 2018 Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act as at 15 May 2018, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience as at 15 May 2018, comprising the May 2018 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 59 above and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience as at 15 May 2018 exposed the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk.

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience as at 15 May 2018 comprised the May 2018 Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act as at 15 May 2018, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience as at 15 May 2018, comprising the May 2018 Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 59 and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience as at 15 May 2018 were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

E. INADEQUACY OF STEPS TAKEN BY RI ADVICE UP TO 12 AND 13 MARCH 2019 AND INADEQUACY OF CYBERSECURITY SYSTEMS IN PLACE AS AT 12 AND 13 MARCH 2019

E.1 First RI Shepparton Cybersecurity Incident – May 2018

61 At all material times, Financial Lifestyle Partners (Shepparton) Pty Ltd and Sandra Miller were and are:

(a) together trading as an RI Advice Practice, RI Advice Shepparton (**RI Shepparton**);

(b) ARs of RI Advice;

(c) not ARs of any other financial services licensee; and

(d) engaged in providing financial services, on RI Advice's behalf, to Retail Clients.

62 At all material times, Sandra Miller was and is a principal and a director of Financial Lifestyle Partners (Shepparton) Pty Ltd.

63 On about 29 May 2018, RI Advice became aware, or ought to have become aware, of a Cybersecurity Incident involving Sandra Miller and RI Shepparton that had occurred on about 23 May 2018 (**First RI Shepparton Cybersecurity Incident**).

Particulars

Email from George Ambrose of RI Advice to ADG Complaints (ANZ) dated 29 May 2018 [RIF.0004.0005.6804].

Notifiable Data Breach Assessment Guide dated 18 June 2018. [FFG.1016.0001.0235].

Further, as to RI Advice's knowledge, the plaintiff refers to and repeats paragraph 16 above.

64 By about 13 September 2018 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the First RI Shepparton Cybersecurity Incident, that it had been reported that:

(i) an unknown party had obtained unauthorised access to Sandra Miller's RI Shepparton email account; and

(ii) the unknown party had used the email account to impersonate Sandra Miller by sending emails to request a bookkeeper to transfer USD50,000 to a Turkish bank account that day (which transfer was not made);

Particulars

RI Advice was provided with copies of the emails exchanged on 23 May 2018 between Sandra Miller's RI Shepparton email account and the bookkeeper [RIF.0004.0005.6804 and RIF.0004.0005.6807].

The ADG Incident Register Incident Data Report [FFG.1016.0001.0004] and the IOOF COR Incident Master Spreadsheet [FFG.1016.00001.1389] both record that the First RI Shepparton Cybersecurity Incident was entered on 30 May 2018 with an incident reference of RE_047922.

(b) had endorsed or allowed the First RI Shepparton Cybersecurity Incident to be recorded in the Aligned Dealer Group Incident Register and the incident had been endorsed by the RI Advice Event Working Group for closure in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by RI Shepparton and RI Advice in respect of the First RI Shepparton Cybersecurity Incident, prior to the incident being endorsed for closure in the Aligned Dealer Group Incident Register, were limited to the following:

(i) RI Advice had advised RI Shepparton to ensure that RI Shepparton's staff were informed of this matter and were to be alert for suspicious emails; to verify all client withdrawal requests with a phone call; and to upgrade RI Shepparton's IT security and set up extra authentication on email accounts;

(ii) RI Shepparton had reported that it had changed 'all' passwords for all staff and had started to use the 'LastPass' password manager to secure all passwords;

(iii) the incident had been registered with ACORN;

(iv) a third-party information technology service provider had reviewed the incident and all of RI Shepparton's computers and had concluded that:

(A) the likely cause was a Trojan (a form of malicious software) installed on Sandra Miller's laptop computer, and the Trojan had been removed;

(B) the unknown actor had access to Sandra Miller's emails and appeared to have read her emails in order to impersonate her, and this email account did not contain client information; and

(C) the unknown actor did not have access to any of RI Shepparton's other computer systems, and these had not been impacted.

Particulars

The various reported matters and steps taken in respect of the First RI Shepparton Cybersecurity incident referred to in sub-paragraphs (a) to (c) above were recorded in the RI Advice Event Working Group Minutes of Forum Meeting #29 dated 13 September 2018 [FFG.1016.0001.0420].

Notifiable Data Breach Assessment Guide [FFG.1016.0001.0235].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

65 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15 and 61 to 64 above, after becoming aware, or after it ought to have become aware, of the First RI Shepparton Cybersecurity Incident and prior to endorsing the closure of the First RI Shepparton Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified the root cause of the First RI Shepparton Cybersecurity Incident;

(b) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the First RI Shepparton Cybersecurity Incident; and

(c) incorporated the findings about the root cause and lessons learnt from the First RI Shepparton Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the First RI Shepparton Cybersecurity Incident:

(A) Cyber training and awareness;

(B) Multi-factor authentication;

(C) Incident response;

(D) Email filtering; and

(E) Application whitelisting;

Particulars

Further details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Cyber training and awareness [ED 6.1 to ED 6.7];

(b) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(c) Incident response [ED 12.1 to ED 12.5];

(d) Email filtering [ED 9.4 and ED 9.8]; and

(e) Application whitelisting [ED 9.2 and ED 9.5].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the First RI Shepparton Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the First RI Shepparton Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 65(a) to (c) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15 and 61 to 64 above,

and at trial ASIC will rely on the Bell Report.

66 RI Advice did not take the steps referred to in paragraph 65 above, adequately or at all, by 12 or 13 March 2019 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 64(c) above, which did not amount to taking the steps referred to in paragraph 65 above adequately or at all.

E.2 RI Advice's receipt of reports in relation to FFG Data Breach

67 On or about 4 June 2018, FFG lodged a Notifiable Data Breach form (**Notifiable Data Breach Form**) in respect of the FFG Data Breach with the Office of the Australian Information Commissioner (**OAIC**), and RI Advice was aware of that fact from about that date.

Particulars

Notifiable Data Breach Form [PP2.0010.0001.0024].

Email from Nikolaos Kloufetos to Peter Ornsby and others dated 22 June 2018 attaching memorandum titled 'Frontier Financial Group Data Breach Remediation Project update' [FFG.0014.0001.0292; FFG.0014.0001.0294].

The RI Advice Event Working Group Forum Meeting #30 papers dated 22 October 2018 [FFG.1016.0001.0544 at 0573 to 0574] noted that on 16 May 2018 the Notifiable Data Breach Assessment was to be completed and reviewed by second line risk and legal, and that on 4 June 2018 the Notifiable Data Breach Form had been submitted to the OAIC.

68 By its Notifiable Data Breach Form, FFG estimated that it was likely that the 833 customers about whom it held high level information were at risk of serious harm as a result of the FFG Data Breach.

69 Between about 5 and 7 June 2018, FFG notified certain of its Retail Clients of the FFG Data Breach, and RI Advice was aware of that fact from about those dates.

Particulars

The notifications were sent by letter dated 5 June 2018, signed by Richard McLean of FFG. A version of the letter is at PP2.0011.0001.0116 [at 0118].

The review and dispatch of the letters was noted by the RI Advice Event Working Group in the Forum Meeting #30 papers dated 22 October 2018 [FFG.1016.0001.0544].

70 On or about 7 August 2018, RI Advice received from FFG a report prepared by a third-party IT service provider, Vixtro, regarding FFG's desktop and network security (**Vixtro Report**).

Particulars

Frontier Financial Group IT Report, dated 3 August 2018 [FFG.1000.0001.0058].

The receipt of the report by RI Advice was noted in the RI Advice, FFG and KPMG Tripartite meeting minutes for 7 August 2018 [FFG.0010.001.5155].

71 By its receipt of the Vixtro Report, RI Advice was aware that Vixtro had reported deficiencies with FFG's desktop and network security, including that:

(a) 90% of desktops were identified as not having up-to-date antivirus software (page 1);

(b) there were no scheduled scans during the working week for antivirus software (page 1);

(c) there was no filtering or quarantining of emails (page 2);

(d) no offsite backups had been performed (page 2);

(e) the domain Administrator account was still default and the password was known by external parties (page 2);

(f) passwords and other security details were found in text files on the server desktop (page 2); and

(g) the remote desktop computer was accessible on default port 3389 (page 2).

72 By about 7 September 2018, RI Advice was aware that 27 Retail Clients of FFG had informed FFG of the unauthorised use of their personal information.

Particulars

The 27 affected Retail Clients of FFG were listed in a client impact spreadsheet dated 7 September 2018 [FFG.0010.0001.5833].

The updated client impact spreadsheet was noted as being available to RI Advice through the 'evidence folder', in the RI Advice, FFG and KPMG Tripartite meeting minutes for 11 September 2018 [FFG.0010.0001.5172].

The communications from affected Retail Clients were kept in FFG files in respect of each client, which files were made available to RI Advice: [PP2.0011.0001.0184, PP2.0011.0001.0131, PP2.0011.0001.0027, PP2.0011.0001.0074, PP2.0011.0001.0116, PP2.0011.0001.0149, PP2.0011.0001.0348, PP2.0011.0001.0170, PP2.0011.0001.0390, PP2.0011.0001.0362, PP2.0011.0001.0041, FFG.0010.0001.0208, PP2.0011.0001.0253, PP2.0011.0001.0216, PP2.0011.0001.0060, PP2.0011.0001.0230, PP2.0011.0001.0002, PP2.0011.0001.0320, PP2.0011.0001.0163, PP2.0011.0001.0269, PP2.0011.0001.0377, PP2.0011.0001.0241, FFG.0010.0001.0551].

E.3 RI Advice's cyber security risk reviews of RI Advice Practices – late 2018

73 In about August 2018, in response to a request from RI Advice, Security in Depth, a third-party cybersecurity firm, provided a proposal to perform a cyber assurance risk review (**CARR**) of 110 RI Advice Practices.

Particulars

Email chain between Peter Ornsby, CEO of RI Advice, and Michael Connory, CEO of Security in Depth, between 10 and 15 August 2018 [RIF.0004.0004.3598], attaching Security in Depth Quotation for supply of Cyber Assurance Risk Rating for RI Group dated 15 August 2018 [RIF.0004.0004.3605].

74 In about September and October 2018, RI Advice engaged Security in Depth to perform a CARR of only five RI Advice Practices, including RI Circular Quay and RI Shepparton.

Particulars

Security in Depth was engaged to perform CARRs of the ARs trading as RI Advice – Berwick (namely Casey FP Pty Ltd, Craig Allan Volk, Pierina Di Stella and Bradley Stephen Poole) (**RI Berwick**), the ARs trading as Horizons Wealth (namely, Matthew John Dunstone, Scott Paul Mitton and The Trustee for Melbourne Wealth Manager Unit Trust) (**Horizons Wealth**), the ARs trading as RI Lower Hunter (namely, Gordon Financial Services Pty Ltd, Gilbert Gordon and Stephen Baxter) (**RI Lower Hunter**), RI Circular Quay, and RI Shepparton.

Email chain between Peter Ornsby and Michael Connory, Security in Depth re Cyber Assurance Risk rating – pilot dated 4 September 2018 [RIF.0004.0004.6492].

Email from Michael Connory, Security in Depth, to Peter Ornsby re Introduction letter dated 7 September 2018 [RIF.0004.004.5457].

Email chain between Peter Ornsby and Brad Poole, RI Berwick, dated 12 September 2018 [RIF.0004.0004.4083].

Email from Peter Ornsby to Gil Gordon, RI Lower Hunter, dated 12 September 2018 [RIF.0004.0004.9119].

Email from Peter Ornsby to Matt Dunston, Horizons Wealth, dated 12 September 2018 [RIF.0004.0004.9191].

Email chain between Peter Ornsby, Sandra Miller, RI Shepparton and Michael Connory dated 22 and 23 October 2018 [RIF.0004.0005.0114].

Email from Peter Ornsby to Sandra Miller, RI Shepparton dated 23 October 2018 [RIF.0004.0004.9209].

Email from Peter Ornsby to John Walker, RI Circular Quay dated 23 October 2018 [RIF.0004.0004.8964].

75 After having completed the CARRs of three RI Advice Practices, in about October 2018, Security in Depth provided RI Advice with a CARR report for the RI Advice Group, by which it informed RI Advice that:

(a) each of the three RI Advice Practices had significant issues with managing and protecting clients' data, and if this was an accurate reflection on the entire RI Advice organisation, significant change would be urgently recommended;

(b) the following critical issues were discovered during Security in Depth's review process:

(i) Poor password management – enabling potential malicious individuals to be able to gain access to client files;

(ii) Limited or poor use of two factor authentication – meaning that once a password was compromised a malicious individual would have no security protocols stopping them from gaining complete access to all systems;

(iii) Limited or non-existent monitoring tools and services to detect if a malicious individual had gained access or still had access to internal systems;

(iv) Limited or no process for maintaining strong governance by implementing and maintaining strong policies and processes;

(v) No processes for managing potential cybersecurity incidents, which Security in Depth considered a serious requirement for staff awareness training; and

(vi) No staff or vendor validation process;

(c) Security in Depth had discovered a malicious attempt to gain access to information, and yet no detection system was in place, no process to manage the incident was available, and no communication process was utilised to provide information concerning, and manage, the incident;

(d) the three RI Advice Practices reviewed were well below industry standards for finance organisations across Australia, and Security in Depth recommended significant changes to process and policy; and

(e) Security in Depth recommended that RI Advice immediately have CARRs performed of all of its RI Advice Practices (**Recommended AR Network CARRs**).

Particulars

The matters referred to in sub-paragraphs (a) to (e) above were referred to in the CARR report for RI Advice, dated October 2018 [FFG.1012.0001.0066] at page 3.

Security in Depth prepared the report after performing the CARRs of RI Lower Hunter, RI Advice Berwick and Horizons Wealth.

76 Between about October and November 2018, Security in Depth also provided RI Advice with CARR reports for five of its RI Advice Practices.

Particulars

CARR report for RI Berwick, dated September 2018 [FFG.1012.0001.0018];

CARR report for Horizons Wealth, dated September 2018 [FFG.1012.0001.0008];

CARR report for RI Lower Hunter, dated October 2018 [FFG.1012.0001.0028];

CARR report for RI Circular Quay, dated October 2018 [FFG.1012.0001.0038]; and

CARR report for RI Shepparton, dated October 2018 [FFG.1012.0001.0048].

77 By reason of its receipt of the five CARR reports referred to in paragraph 76 above, RI Advice was aware that Security in Depth considered that:

(a) three of the five RI Advice Practices' cybersecurity status was assessed as 'Poor' (including RI Circular Quay and RI Shepparton);

(b) the other two of the five RI Advice Practices' cybersecurity status was assessed as 'Fair'; and

(c) in relation to the three RI Advice Practices the cybersecurity status of which was assessed as 'Poor':

(i) they had no discernible cybersecurity policies, processes and procedures in writing, and all policies that did exist had been put together to manage immediate security requirements rather than being based on an overarching security framework;

(ii) they had no structured cybersecurity governance program driven from the executive down; and

(iii) it was highly likely that a cyber incident could occur over the next twelve months with significant impact on their ability to provide critical services.

Particulars

RI Berwick's cybersecurity status was assessed as 'Poor'. The matters referred to above relating to RI Berwick were reported in the CARR report for RI Berwick, dated September 2018 [FFG.1012.0001.0018] at page 3.

Horizons Wealth's cybersecurity status was assessed as 'Fair': CARR report for Horizons Wealth, dated September 2018 [FFG.1012.0001.0008] at page 3.

RI Lower Hunter's cybersecurity status was assessed as 'Fair': CARR report for RI Lower Hunter, dated October 2018 [FFG.1012.0001.0028] at page 3.

The matters referred to above relating to RI Circular Quay were reported in the CARR report for RI Circular Quay, dated October 2018 [FFG.1012.0001.0038] at page 3.

The matters referred to above relating to RI Shepparton were reported in the CARR report for RI Shepparton, dated October 2018 [FFG.1012.0001.0048] at page 3.

78 Further, by about 25 January 2019 at the latest, RI Advice received from Cyber Indemnity Solutions, a third-party cybersecurity firm, a summary of its cybersecurity assessment for two RI Advice Practices.

Particulars

Cyber Assessments for Retire Invest Bondi and for Retire Invest Newcastle & Lower Hunter (undated) [FFG.1012.0001.0058].

RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003] (item 3).

As referred to in paragraph 102(a) below, in about April 2019, RI Advice received detailed assessments of the Cyber Indemnity Solutions cybersecurity assessment for the two RI Advice Practices.

79 By reason of its receipt of the cybersecurity assessment summary referred to in paragraph 78 above, RI Advice was aware that Cyber Indemnity Solutions considered that:

(a) one of the two RI Advice Practices' cybersecurity status was assessed as 'Basic/Adhoc', and the cybersecurity status of the second RI Advice Practice was assessed as 'Maturing'; and

Particulars

Retire Invest Bondi's cybersecurity status was assessed as 'Basic/Adhoc' (page 2).

Retire Invest Newcastle & Lower Hunter's cybersecurity status was assessed as 'Maturing' (page 4).

(b) in relation to the RI Advice Practice the cybersecurity status of which was assessed as 'Basic/Adhoc':

(i) identification and management of IT assets was not performed. When organisations do not know what they have it is very difficult to protect systems and access because management is ad-hoc at best (page 3);

(ii) there was no coordination with third party suppliers to manage cyber risk in respect of supply chain risk (page 3);

(iii) access control was not performed to a sufficient standard. There were weak passwords, regular users had administration access and weak authentication was common (page 3);

(iv) there was no protection of data. The organisation did not manage information and records to any appropriate standard (page 3);

(v) application hardening and white listing was not performed. This left the organisation vulnerable to many hacking exploits (page 3);

(vi) there was no proactive monitoring of cyber risk with protective technologies (page 3);

(vii) there was no continuous monitoring of cyber threats. There were no monitoring capabilities to detect cybersecurity breaches caused by vulnerabilities (page 3); and

(viii) there were no daily backups performed (page 3).

80 Other than as referred to in paragraphs 76 to 79 above, RI Advice did not obtain the Recommended AR Network CARRs by 12 or 13 March 2019 and nor, other than as referred to in paragraph 117(i) below, did it do so at any relevant time.

E.4 KPMG report in relation to the FFG Data Breach

81 On or about 12 July 2018, ANZ, on behalf of RI Advice, engaged KPMG Forensic Pty Ltd (**KPMG**) to perform a forensic technology investigation in respect of the FFG Data Breach.

Particulars

Letter from KPMG to Nikolas Kloufetos, ANZ, dated 10 July 2018 and signed by ANZ on 12 July 2018 [FFG.0015.0001.8906].

RI Advice's event closure report for the FFG Data Breach dated 18 September 2019 [FFG.1020.0001.0154] refers at pages 1 to 2 to RI Advice's engagement of KPMG.

82 On or about 24 October 2018, KPMG provided RI Advice with a report setting out its conclusions and recommendations from its investigation of the FFG Data Breach (**KPMG Report**).

Particulars

KPMG Retire Invest Pty Ltd Cyber Incident Response – Forensic Review dated 24 October 2018 [PP2.1003.0002.0004].

Appendix A – Grant Thornton Incident assessment Frontier FG [PP2.1003.0001.0026].

Appendix B - Jayden RDP Sessions [PP2.1003.0001.0032].

Appendix C - Internet Sites Visited [PP2.1003.0001.0042].

Appendix D - Dropbox Files Accessed [PP2.1003.0001.0056].

Appendix E - Artefacts Relating to Frontier File Share Access [PP2.1003.0001.0058].

Appendix F – Frontier Security Implementation Schedule [RIF.0004.0005.5290] (Draft).

Appendix G – Essential Eight maturity levels dated April 2018 [RIF.0004.0005.5287].

83 By its receipt of the KPMG Report, RI Advice was aware that KPMG had concluded that:

(a) the root cause of the FFG Data Breach was likely to be the result of the malicious user performing a brute force attack (that is, attempting login by trial and error) using an FFG employee login against FFG's remote desktop server (at [1.3]);

(b) between 20 and 30 October 2017, there were 27,814 unsuccessful login attempts using 2,178 different usernames from 10 different countries (at [2.1]);

(c) there was a lack of working backups of the compromised remote desktop server, which meant that potential evidence regarding the FFG Data Breach for the period between 30 December 2017 and 3 March 2018 was unable to be recovered for analysis (at [1.4] and [2.1]);

(d) on a conservative basis, the malicious user had spent in excess of 155 hours logged into the FFG infrastructure across a span of 106 days from 30 December 2017 to 15 April 2018 (at [1.3] and [2.2]);

(e) the malicious user 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 (at [2.2]);

(f) the malicious user had access through the compromised FFG user's account to the entire contents of FFG's file server, including documents relating to three FFG clients who were the subject of reported instances of identity fraud in April 2018 (at [1.3] and [2.2.2]);

(g) given the extent of the period of compromise and the free access to all contents of both file server data shares, all data on FFG's data services should be considered to be compromised (at [1.3] and [2.2.1]); and

(h) KPMG recommended that:

(i) all data on the fileserver shares that were accessible during the period that the malicious user had access be reviewed for personally identifiable information or other sensitive information that may indicate the issue was classified as a notifiable data breach (at [3]);

(ii) 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 (at [3]); and

(iii) a review of the disaster recovery back-up process should be conducted to identify the cause which rendered the incremental backups unusable for KPMG's analysis, which review should encompass both the onsite and cloud backups (at [3]).

E.5 Inadequacy of steps taken by RI Advice up to 12 and 13 March 2019

84 As at 12 and 13 March 2019, FFG and RI Advice had not concluded their investigation and remediation of the FFG Data Breach.

Particulars

As referred to in paragraph 96 below, FFG and RI Advice did not conclude their investigation and remediation until about September 2019.

'Event Closure Report – RI Advice: Frontier Financial Group (FFG) Notifiable Data Breach (NBD) – FINAL' dated 18 September 2019 – [FFG.1020.0001.0154].

Email dated 19 September 2019 from Richard McLean, of FFG, to OAIC, copied to Nikolas Kloufetos, Project manager, Licensee Remediation, IOOF, re OAIC Reference number: DBN18/00331 – Conclusion of investigation and remediation of Frontier Financial Group data breach [FFG.1020.0001.0206].

85 From about September and October 2018 to 13 March 2019, including as a consequence of its knowledge of the FFG Data Breach, RI Advice had planned and/or undertaken the following cybersecurity initiatives to address cybersecurity issues across its AR network and to reduce the risk of a Cybersecurity Incident occurring (**March 2019 Cybersecurity Initiatives**):

(a) engaging external security consultancy firms Security in Depth and Cyber Indemnity Solutions to conduct cybersecurity reviews of six RI Advice Practices (**Six CARRs**).

(b) inclusion of cybersecurity as a risk management discussion topic within the RI Advice Proprietors Advisory Council (**PAC**), Risk and Event Forum and Event Working Group Forum (**Cybersecurity Discussion Topics**);

(c) beginning of development or update of a number of core cybersecurity documents including standards, guides and procedures with the assistance of Security in Depth (**Documentation Update**);

(d) mandating attestations from ARs as to cyber fraud capabilities and local area network cyber fraud protections (**Attestations on Cyber Capabilities and Protections**);

(e) establishing cyber awareness and training material, including draft cyber security standard questions relating to the cyber awareness material (**Awareness Material**);

(f) mandating the use of multi-factor authentication on Xplan (a database that held Personal Information) and local area networks (**Mandated MFA**);

(g) mandating the use of a password manager and password encryption of email correspondence that included Personal Information (**Mandated Password Management**);

(h) reviewing the implementation of a Cyber Standard (**Review of Cyber Standard**);

(i) implementing training modules relating to ISO 27001 and Australian Signals Directorate (**ASD**) Essential Eight policy and procedure development (**Training Implementation**); and

(j) offering a cyber insurance solution to the network of RI Advice ARs (**Cyber Insurance**).

Particulars

RI Advice letter to ASIC dated 19 December 2018 [FFG.1015.0001.0003].

RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003].

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062]

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003]

RI Advice letter to ASIC dated 28 November 2019 [FFG.1023.0001.0003]

Further particulars of the matters pleaded in sub-paragraphs (a) to (j) above are provided in paragraph 87 below.

86 As at 12 and 13 March 2019, RI Advice had not planned or implemented any initiatives for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 85 above.

87 As at 12 and 13 March 2019, RI Advice had only implemented the March 2019 Cybersecurity Initiatives to the extent referred to below:

(a) in respect of the Six CARRs, cyber security assessments had been performed on six RI Advice Practices, but RI Advice had not received detailed reports for the cybersecurity assessments for one of those practices;

Particulars

RI Advice had received Security in Depth CARR reports for the five RI Advice Practices referred to in paragraph 76 above and the Cyber Indemnity Solutions cyber assessment summary for the two RI Advice Practices referred to in paragraph 78 above (one of which (RI Advice Lower Hunter) had also been assessed by Security in Depth as referred to in paragraph 76 above).

Data Protect Cyber Risk Assessment for RI Advice Bondi dated about 12 March 2019 [FFG.1014.0002.0232] and supporting documents [FFG.1014.0002.0203, FFG.1014.0002.0212, FFG.1014.0002.0221, FFG.1014.0002.0246, FFG.1014.0002.0254, FFG.1014.0002.0264, FFG.1014.0002.0275, FFG.1014.0002.0286, FFG.1014.0002.0297, FFG.1014.0002.0310, FFG.1014.0002.0319, FFG.1014.0002.0330, FFG.1014.0002.0347; FFG.1014.0002.0356, FFG.1014.0002.0367, FFG.1014.0002.0375, FFG.1014.0002.0388, FFG.1014.0002.0396, FFG.1014.0002.0406].

As detailed in paragraph 102(a) below, RI Advice did not receive the detailed cybersecurity assessments performed by Cyber Indemnity Solutions for RI Advice Lower Hunter until about 15 April 2019.

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062], items 1, 2 and 3.

(b) the Cybersecurity Discussion Topics had been implemented at the PAC and the RI Event Working Group;

Particulars

The PAC, which included a group of AR representatives, met with RI management on a quarterly basis: RI Advice letter to ASIC dated 28 November 2019 [FFG.1023.0001.0003].

RI Advice Proprietors Advisory Council PAC Meeting agenda dated 21 and 22 February 2019 [FFG.1026.0001.0166]; minutes dated 21 and 22 May 2019 [FFG.1026.0001.0159]; and minutes dated 30 and 31 July 2019 [FFG.1026.0001.0006].

(c) The RI Event Working Group involving RI Advice and IOOF included discussions of cybersecurity related risks [FFG.1016.0001.0699] (Minutes dated 22 October 2018).the Documentation Update was planned for 31 March 2019 but was incomplete;

Particulars

RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003], item 3(b).

As at 11 March 2019, RI Advice was working with Security in Depth to update the proposed 'security policies and procedures': RI Report 11 March 2019 [FFG.1022.0001.2732] (page 2).

(d) the Attestations on Cyber Capabilities and Protections had not been implemented, and were due to be implemented on 30 June and 30 September 2019;

Particulars

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062], item 4(ii).

(e) Awareness Material had commenced being implemented in February 2019 through the delivery of cybersecurity awareness webinars to ARs run by Security in Depth, but was incomplete;

Particulars

Implementation of an updated network cyber education program with Security in Depth started in February 2019: RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003], item 3(b), RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062], item 4(ii).

The February 2019 webinars were referred to in the RI Report 11 February 2019 [FFG.1022.0001.2643] and the RI Report 11 March 2019 [FFG.1022.0001.2732].

Draft cyber security standard questions relating to the cyber awareness material had yet to be developed.

(f) Mandated MFA was planned for 31 March 2019 but was incomplete;

Particulars

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062], item 4(ii).

As at 11 March 2019, RI Advice had evaluated and short-listed different password management solutions and was investigating whether they supported two-factor authentication: RI Report 11 March 2019 [FFG.1022.0001.2732].

(g) Mandated Password Management was planned for 31 March 2019 but was incomplete;

Particulars

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062], item 4(ii).

As at 11 March 2019, RI Advice had evaluated and short-listed different password management solutions and was investigating whether they supported two-factor authentication, and had met with

LastPass which had offered a commercial arrangement: RI Report 11 March 2019 [FFG.1022.0001.2732] (page 1 and 2).

(h) the Review of the Cyber Standard was planned for 31 March 2019 but was incomplete;

Particulars

RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003], item 3(b).

As at 11 March 2019, RI Advice was 'working through' and updating the proposed security policies and procedures: RI Report 11 March 2019 [FFG.1022.0001.2732] (page 2).

(i) Training Implementation had commenced from February 2019 but was incomplete; and

Particulars

The training implemented as at 11 March 2019 is referred to in sub-paragraph (e) above.

(j) Cyber Insurance had been obtained and was being offered to ARs.

Particulars

IOOF Cyber Insurance Solution - Feb 2019 Final, February 2019, [FFG.1020.0001.0108].

RI Advice letter to ASIC dated 19 December 2018 [FFG.1015.0001.0003].

As at 11 March 2019, two RI Advice Practices had taken up the cyber insurance: RI Report 11 March 2019 [FFG.1022.0001.2732] (page 1).

88 Further to paragraphs 85 and 87 above, following the change of ownership of RI Advice from ANZ to IOOF in October 2018, from about October 2018, RI Advice replaced some of the May 2018 Documentation and Controls that it

held or had access to, and which had been developed by ANZ, with IOOF-developed documentation (**IOOF Developed Documentation**).

Particulars

The IOOF Developed Documentation which RI Advice held or had access to from about October 2018 is set out in Schedule C.

E.6 Inadequacy of March 2019 Cybersecurity Documentation and Controls

89 As at 12 and 13 March 2019, the Cybersecurity Documentation and Controls that RI Advice held or had access to for the management of risk in respect of cybersecurity and cyber resilience across its AR network were as follows:

(a) the May 2018 Documentation and Controls referred to in paragraphs 57(g) and (r) above;

(b) the IOOF Developed Documentation;

Particulars

The IOOF Developed Documentation which RI Advice held or had access to as at 12 and 13 March 2019 is set out in Schedule C.

(c) Practice Servicing Assessment for Frontier dated 14 September 2018 [FFG.1007.0001.0081];

(d) RI Advice procedures, application forms and checklists for recruitment, appointment and cancellation of ARs; and

Particulars

The documents referred to in paragraph 57(q) above (with the exception of the ADG Recruitment Fact Find (Version 15) dated February 2018 [FFG.1022.0001.2377]; RI Advice Authorised Representative Application Form, Version 18, April 2018 [FFG.1022.0001.1679]; and RI Advice Practice Application Form Version 14, May 2017 [FFG.1022.0001.1702]).

APPOINTMENT: Practice Appointment Checklist (CAR or Sole Trader) dated about 29 November 2018 [FFG.1022.0001.1771].RI Advice Group Practice Application Form (version 16) dated 1 October 2018 [FFG.1022.0001.1731].

RI Advice Authorised Representative Application Form (Version 19) dated October 2018 [FFG.1022.0001.1775].

APPOINTMENT: Authorised Representative Appointment Checklist dated about June 2016 [FFG.1022.0001.1773].

(e) presentations, webinars and newsletters covering cybersecurity awareness related topics;

Particulars

APRA Cyber Security Legislation – CPS 234 dated 20 February 2019 [FFG.1022.0001.3462].

1.6 - Notifiable Data Breach Reconnect Conference August 2018 FINAL.pptm dated 1 August 2018 [FFG.1022.0001.2618].

Quarterly Video links (October 2018 and March 2019] [FFG.1022.0001.2822].

RI Report 24 September 2018 [FFG.1022.0001.2688].

RI Report 8 October 2018 [FFG.1022.0001.2799].

RI Report 15 October 2018 [FFG.1022.0001.2744].

RI Report 5 November 2018 [FFG.1022.0001.2704].

RI Report 12 November 2018 [FFG.1022.0001.2739].

RI Report 19 November 2018 [FFG.1022.0001.2755].

RI Report 26 November 2018 [FFG.1022.0001.2779].

RI Report 29 January 2019 [FFG.1022.0001.2710].

RI Report 4 February 2019 [FFG.1022.0001.2809].

RI Report 11 February 2019 [FFG.1022.0001.2643].

RI Report 18 February 2019 [FFG.1022.0001.2666].

RI Report 11 March 2019 [FFG.1022.0001.2732].

(f) Services and Resources Support Agreement between IOOF and RI Advice;

Particulars

Services and Resources Support Agreement between IOOF Service Co Pty Ltd and members of the IOOF Group dated 5 July 2017 [RIF.0003.0090.0085].

Deed of Amendment to the Services and Resources Support Agreement between IOOF Service Co Pty Ltd, RI Advice Group Pty Ltd and others dated 1 October 2018 [RIF.0003.0090.0124].

(g) CARR reports and reports in respect of Cybersecurity Incidents;

Particulars

The Vixtro Report referred to in paragraph 70 above and the particulars thereto.

The CARR reports referred to in paragraph 75(e) and 76 above and the particulars thereto.

The KPMG Report referred to in paragraph 82 above and the particulars thereto.

The CARR report referred to in paragraph 87(a) above and the particulars thereto.

(h) minutes of PAC and RI Event forum and Working Groups meetings; and

Particulars

The minutes of meetings referred to in paragraph 87(b) above and the particulars thereto.

The RI Risk and Event Forum Minutes [FFG.1016.0001.0711] (Minutes dated 29 October 2018); RI Advice Event Working Group Forum #4 (Minutes dated 20 February 2019) [FFG.1016.0001.1137].

(i) quotations for the supply of cybersecurity training and support services;

Particulars

Quotations dated 19 November 2018 [RIF.0004.0004.7561]; 12 December 2018 [RIF.0004.0004.2966] and [RIF.0006.0015.0001]; 15 January 2019 [RIF.0004.0004.2749].

(the **March 2019 Documentation and Controls**).

90 As at 12 and 13 March 2019, RI Advice did not have in place any Cybersecurity Documentation and Controls for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 89 above.

91 By its March 2019 Documentation and Controls, as at 12 and 13 March 2019, RI Advice:

(a) did not adequately document the roles and responsibilities of RI Advice and its ARs as to the management of risk in respect of cybersecurity and cyber resilience across its AR network;

(b) predominantly relied upon the IOOF Developed Documentation, which:

(i) in many cases pre-dated IOOF's acquisition of RI Advice;

(ii) was specific to the IOOF organisation and its IT environment;

(iii) was not tailored to RI Advice and its ARs' requirements for the management of risk in respect of cybersecurity and cyber resilience across its AR network; and

(iv) had not been implemented and operationalised by RI Advice as part of, or was not relevant to, its governance and management of risk in respect of cybersecurity and cyber resilience across its AR network;

Particulars

The IOOF Developed Documentation which RI Advice held or had access to as at 12 and 13 March 2019 which had the characteristics referred to in sub-paragraphs (i) to (iv) above is set out in Schedule C.

(c) did not adopt and implement adequate Cybersecurity Documentation and Controls in each of the 13 Cybersecurity Domains;

(d) did not meet the Minimum Cybersecurity Requirements; and

(e) did not adequately manage risk in respect of cybersecurity and cyber resilience across its AR network.

Particulars

In respect of sub-paragraphs (a), (c), (d) and (e) above, the gaps between the March 2019 Documentation and Controls and the Cybersecurity Documentation and Controls which RI Advice should have had in place in each of the 13 Cybersecurity Domains in order to meet the Minimum Cybersecurity Requirements are set out in Schedule D.

RI Advice was required to have Cybersecurity Documentation and Controls in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network. The obligation was upon RI Advice.

The Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum

Cybersecurity Requirements should have adequately addressed each of the 13 Cybersecurity Domains by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

RI Advice should have had each of the Cybersecurity Documentation and Controls specified in Schedules A and D in place in each of the 13 Cybersecurity Domains prior to and as at 12 and 13 March 2019 in order to meet the Minimum Cybersecurity Requirements by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 to 15 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

E.7 Contraventions in respect of conduct up to, or as at, 12 and 13 March 2019

92 By reason of the matters pleaded in paragraphs 2 to 5, 11 to 15, 21, 22, 25, 26, 31, 32, 36, 37, 41, 42, 49, 50, 57 to 59, 65, 66, 85 to 91 above:

(1) at all times from 15 May 2018 to 12 March 2019; alternatively

(2) on 12 March 2019,

RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, by reason of:

(i) the conduct pleaded in paragraph 59 above and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above;

(ii) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above; and/or

(iii) the conduct pleaded in paragraph 66 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 61 to 65 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that the public is entitled to expect, at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, by reason of:

(i) the conduct referred to in paragraph 59 above and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity

Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above;

(ii) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above; and/or

(iii) the conduct pleaded in paragraph 66 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 61 to 65 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws are detailed in paragraphs 13 to 15 above and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 92(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 92(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 92(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 92(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times from 15 May 2018 comprised the May 2018 Documentation and Controls and as at 12 March 2019, comprised the March 2019 Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience from 15 May 2018, comprising the May 2018 Documentation and Controls and as at 12 March 2019, comprising the March 2019 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of:

(i) the conduct pleaded in paragraph 59 above, and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the

respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above; and/or

(ii) the conduct pleaded in paragraph 91 above, and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, exposed the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk.

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times from 15 May 2018 comprised the May 2018 Documentation and Controls and as at 12

March 2019, comprised the March 2019 Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience comprising from 15 May 2018, the May 2018 Documentation and Controls, and as at 12 March 2019, the March 2019 Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of:

(i) the conduct pleaded in paragraph 59 above, and Schedule B, in that its May 2018 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule B, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 57 and 58 above; and/or

(ii) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times from 15 May 2018 to 12 March 2019, alternatively on 12 March 2019, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

93 Further, by reason of the matters pleaded in paragraphs 2 to 5, 11 to 15 and 85 to 91 above, including with knowledge of the matters in respect of the

Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above, on 13 March 2019, RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act on 13 March 2019, by reason of the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, on 13 March 2019, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that

the public is entitled to expect, on 13 March 2019, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act on 13 March 2019, by reason of the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the

financial services laws are detailed in paragraphs 13 to 15 above and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 93(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 93(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 93(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 93(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience on 13 March 2019 comprised the March 2019 Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act on 13 March 2019, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience as at 13 March 2019, comprising the March 2019 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience on 13 March 2019, exposed the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience on 13 March 2019 comprised the March 2019 Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act on 13 March 2019, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience comprising the March 2019 Documentation and Controls were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience on 13 March 2019 were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

(f) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (a), (d) and (e) above, contravened s 912A(5A) of the Act.

F. INADEQUACY OF STEPS TAKEN BY RI ADVICE UP TO 1 NOVEMBER 2019 AND INADEQUACY OF CYBERSECURITY SYSTEMS IN PLACE AS AT 1 NOVEMBER 2019

F.1 Empowered Cybersecurity Incident – August 2019

94 At all material times until about 27 March 2020, Empowered Financial Partners Pty Ltd (**Empowered**) was:

(a) an AR of RI Advice;

(b) not an AR of any other financial services licensee; and

(c) engaged in providing financial services, on RI Advice's behalf, to Retail Clients on behalf of RI Advice.

95 On or about 23 August 2019, RI Advice became aware of a Cybersecurity Incident that month involving the compromise of an Empowered staff member's email (**Empowered Cybersecurity Incident**).

Particulars

Incident Report dated 23 August 2019 attached to letter dated 27 August 2019 [FFG.1029.0001.0040].

Email from Jeannette McShane, RI Advice to IOOF Advice Risk, re Incident – Cyber Breach dated 23 August 2019, summarising information provided by Bernie Cooney of Empowered, forwarded by Wen Li Zhou, Incident Manager at IOOF to Peter Ornsby, CEO of RI Advice and others [FFG.1029.0001.0028].

As referred to in paragraph 107 below, RI Advice endorsed or allowed the Empowered Cybersecurity Incident to be closed in the Aligned Dealer Group Incident Register by November 2019.

F.2 Inadequacy of steps taken by RI Advice in respect of FFG Data Breach

96 In about September 2019, FFG and RI Advice concluded their investigation and remediation of the FFG Data Breach, as a result of which:

(a) the investigation had revealed that there were 8,104 Retail Clients potentially exposed to the FFG Data Breach;

(b) FFG had, by then, notified 7,366 Retail Clients of the FFG Data Breach and had published a notice on its website in order to notify any others; and

(c) FFG had notified the Australian Taxation Office in respect of Retail Clients whose tax file numbers were held on its files.

Particulars

'Event Closure Report – RI Advice: Frontier Financial Group (FFG) Notifiable Data Breach (NBD) – FINAL' dated 18 September 2019 – [FFG.1020.0001.0154].

RI Advice letter to ASIC dated 4 October 2019 [FFG.1015.0003.0002].

97 On or about 19 September 2019, FFG informed the OAIC, and RI was aware, or ought to have become aware, of the matters referred to in paragraph 96 above.

Particulars

Email dated 19 September 2019 from Richard McLean, of FFG, to OAIC, copied to Nikolas Kloufetos, Project manager, Licensee Remediation, IOOF, re OAIC Reference number: DBN18/00331 – Conclusion of investigation and remediation of Frontier Financial Group data breach [FFG.1020.0001.0206].

RI Advice letter to ASIC dated 4 October 2019 [FFG.1015.0003.0002].

98 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15, 51 to 56, 67 to 72, 81 to 84, 96 and 97 above, after becoming aware of the FFG Data Breach, and with knowledge of the matters in respect of the Cybersecurity

Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 73 to 80 above, by 30 September 2019, alternatively 1 November 2019, RI Advice should have:

(a) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the FFG Data Breach referred to in paragraphs 52 and 83(a) above and as a result of any review conducted to identify the cause of the failure of FFG's disaster recovery backup process as recommended by KPMG and referred to in paragraph 83(h) above; and

(b) incorporated the findings about the root cause and lessons learnt from the FFG Data Breach into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the FFG Data Breach:

(A) Privilege management;

(B) Multi-factor authentication;

(C) Password complexity;

(D) Password management;

(E) Account lockout;

(F) Application whitelisting;

(G) Port security;

(H) Web filtering;

(I) Security and compliance score for Microsoft Office 365;

(J) Antivirus protection;

(K) Log monitoring controls;

(L) Incident response;

(M) Backups; and

(N) Holistic cybersecurity framework.

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Privilege management [ED 5.3 and ED 5.5];

(b) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(c) Password complexity [ED 5.1 and ED 7.1];

(d) Password management [ED 5.1 and ED 7.1];

(e) Account lockout [ED 5.3];

(f) Application whitelisting [ED 9.2 and ED 9.5];

(g) Port security [ED 9.4 and ED 9.8];

(h) Web filtering [ED 9.4 and ED 9.8];

(i) Security and compliance score for Microsoft Office 365 [ED 9.1];

(j) Antivirus protection [ED 10.5];

(k) Log monitoring controls [ED 10.1 to ED 10.6];

(l) Incident response [ED 12.1 to ED 12.5];

(m) Backups [ED.13.3 and ED.13.5]; and

(n) Holistic cybersecurity framework [ED 1.1].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the FFG Data Breach which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the FFG Data Breach, RI Advice should have taken the steps pleaded in paragraphs 98(a) and (b) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15, 51 to 56, 67 to 72, 81 to 84, 96 and 97 above,

and at trial ASIC will rely on the Bell Report.

99 RI Advice did not take the steps referred to in paragraph 98 above adequately by 1 November 2019 or at any relevant time.

Particulars

The steps which RI Advice had taken by 1 November 2019 referred to in paragraphs 100 and 102 below did not amount to taking the steps in respect of cybersecurity and cyber resilience across its AR network referred to in paragraph 98 above adequately.

F.3 Inadequacy of steps taken by RI Advice up to 1 November 2019

100 By 1 November 2019, RI Advice had planned and/or undertaken the following cybersecurity initiatives to address cybersecurity issues across its AR network

and to prevent and manage Cybersecurity Incidents (**November 2019 Cybersecurity Initiatives**):

(a) Six CARRs;

(b) Cybersecurity Discussion Topics;

(c) Documentation Update;

(d) Attestations on Cyber Capabilities and Protections;

(e) Awareness Material;

(f) Mandated MFA;

(g) Mandated Password Management;

(h) development of specific roles and teams to manage Cybersecurity Incidents, such as a 'Head of IT Cyber Security' (**Cybersecurity Leadership**);

(i) a formal cybersecurity gap analysis of ARs to help understand what improvements can be made to RI Advice's current systems and process (**Gap Analysis**);

(j) Review of Cyber Standard;

(k) formalisation of the Cybersecurity Incident Response Plan Breach Process Guide (**Cybersecurity Incident Response Plan Finalisation**);

(l) Training Implementation; and

(m) Cyber Insurance.

Particulars

RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003].

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062].

RI Advice letter to ASIC dated 4 October 2019 [FFG.1015.0003.0002].

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003].

RI Advice letter to ASIC dated 28 November 2019 [FFG.1023.0001.0003].

Further particulars of the matters pleaded in sub-paragraphs (a) to (m) above are provided in paragraph 102 below.

101 As at 1 November 2019, RI Advice had not planned or implemented any initiatives for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 100 above.

102 As at 1 November 2019, RI Advice had only implemented the November 2019 Cybersecurity Initiatives to the extent referred to below:

(a) the Six CARRs were complete;

Particulars

In addition to the matters referred to in paragraph 87(a) above, RI Advice received detailed 'Data Protect' cyber assessments for the two RI Advice Practices referred to in paragraph 78 above by about 15 April 2019.

Email from Sascha Warner, IOOF, to ASIC dated 15 April 2019 [FFG.1014.0002.0001].

Data Protect Cyber Risk Assessment for RI Advice Lower Hunter dated about 10 April 2019 [FFG.1014.0002.0003] and supporting documents [FFG.1014.0002.0013, FFG.1014.0002.0021, FFG.1014.0002.0028, FFG.1014.0002.0037, FFG.1014.0002.0045, FFG.1014.0002.0052, FFG.1014.0002.0059, FFG.1014.0002.0069, FFG.1014.0002.0079, FFG.1014.0002.0088, FFG.1014.0002.0099, FFG.1014.0002.0107, FFG.1014.0002.0116, FFG.1014.0002.0127,

FFG.1014.0002.0136, FFG.1014.0002.0145, FFG.1014.0002.0152, FFG.1014.0002.0158, FFG.1014.0002.0164, FFG.1014.0002.0172, FFG.1014.0002.0179, FFG.1014.0002.0188, FFG.1014.0002.0195].

CARR Report - RI Advice Lower Hunter - July 2019 [FFG.1026.0001.0181]

(b) the Cybersecurity Discussion Topics had been implemented at the PAC, the EWG Forum and the RI Event Working Group;

(c) the Documentation Update was incomplete, but RI Advice:

(i) was developing the Cybersecurity Documents and Controls referred to in paragraphs 103(d) and (e) below, which as referred to in those paragraphs had not been finalised, approved or released;

(ii) had developed the Cybersecurity Documents and Controls referred to in paragraph 103(f) below;

(iii) had developed the Cyber Security RI Mandatory Requirements Checklist dated 29 October 2019 [FFG.1022.0001.0421];

(iv) had developed the Cybersecurity Kaplan questions dated about 10 October 2019 [FFG.1022.0001.2561]; and

(v) had developed the RI Advice Practice attestations on implementation of password management and two factor authentication;

Particulars

AR Responses (13) to questions on implementation of password management and two factor authentication [spreadsheet] dated about 9 October 2019 [FFG.1022.0001.3521].

(d) the Attestations on Cyber Capabilities and Protections had not been implemented and were not expected to be completed until the first quarter of 2020;

Particulars

On 1 November 2019, RI Advice reported that:

1) in November 2019, the new Cyber Security Support Guide [RIF.0006.0001.0001] would be sent to each RI Advice Practice, and each practice's technical provider would attest that the practice conformed to the (ten) initiatives outlined in the guide; and

2) RI Advice had not as yet conducted an audit, assessment or review of its ARs to gain assurance that the Cyber Security Support Guide and email encryption had been implemented and operationalised, but this initiative would 'be undertaken in the first quarter of 2020'.

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], items 2, 6(c) and (j).

(e) Awareness Material had commenced being implemented but remained incomplete;

Particulars

RI Advice had developed training programs on two factor authentication, appropriate password management and password encryption of emails that may contain Personal Information: RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], item 2.

As at 1 November 2019, RI Advice had recorded that 110 ARs had completed the 'Cyber Fraud' or 'Cyber Security Training Essentials' training sessions between about 2 May and 20 August 2019 and 88 ARs had not yet completed this training [FFG.1022.0001.3474].

Draft cyber security standard questions relating to the cyber awareness material had yet to be developed.

(f) Mandated MFA had commenced being implemented;

Particulars

Two factor authentication had been implemented for two applications used by ARs, namely Xplan and DocuSign, including the preparation of a guide how to set up 2FA in Xplan [RIF.0006.0002.0037]. RI Advice had not performed testing to ensure the design and operational effectiveness of the two factor authentication in Xplan. An audit of Xplan users for the implementation of two factor authentication was planned for December 2019. RI Advice was not testing ARs' systems (other than Xplan) for the implementation of two factor authentication: RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], items 6(g) and (h).

90 RI Advice Practices had attested that they had implemented two factor authentication into both Xplan and their local area network (if that local area network contained client personal information), but 7 RI Advice Practices had not provided this attestation: Practice Password Management and 2FA Review spreadsheet [FFG.1022.0001.3521]. 486 ARs and support staff members had attested that they had activated two factor authentication and 5 ARs and support staff had not provided this attestation: AR attestation responses relating to MFA [FFG.1021.0002.0008].

2019-06-12-2FA spreadsheet dated about June 2019 [FFG.1022.0001.3475].

(g) Mandated Password Management was practically complete, however no testing had taken place to monitor its implementation;

Particulars

RI Advice had provided ARs with the LastPass password management system, however RI Advice had not undertaken a testing process to monitor which ARs were using and updating the system: RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], item 6(i).

95 RI Advice Practices had attested that they had implemented an approved online password manager, and 2 RI Advice Practices had not provided this attestation. 93 RI Advice Practices had attested that all documents being sent to clients that hold client personal information by email were password protected, and 4 RI Advice Practices had not provided this attestation: Practice Password Management and 2FA Review spreadsheet [FFG.1022.0001.3521].

(h) Cybersecurity Leadership was a planned initiative which was 'ongoing';

Particulars

No date was provided for the implementation of this initiative: RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], item 4 (page 4).

(i) the Gap Analysis had not been implemented and was planned for the first quarter of 2020;

Particulars

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], item 4 (page 4).

(j) the Review of the Cyber Standard was planned for the end of 2020;

Particulars

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], items 2 and 6(j).

(k) the Cybersecurity Incident Response Plan Finalisation was incomplete, the document was in draft form only and it was expected that the document would achieve a 'final draft status' by the end of November 2019;

Particulars

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], items 2 and 6(j).

(l) Training Implementation had commenced, but was incomplete; and

Particulars

New advisers joining RI Advice were required to complete RI Advice's prescribed cybersecurity training program within three months of joining RI Advice.

RI Advice planned, as part of its November 2019 training program, to provide a document to its ARs to ask them to have their local technician sign off that their local area network met the standard: RI Advice letter to ASIC dated 4 October 2019 [FFG.1015.0003.0002].

No training modules relating to ISO 27001 and ASD Essential Eight policy and procedure development had been completed.

The training implemented as at 1 November 2019 is referred to in sub paragraph (e) above.

(m) Cyber Insurance had been obtained and was being offered to ARs.

Particulars

IOOF Specialist Services Presentation (Multiple pages), 'IOOF Cyber Insurance Solution - Feb 2019 Final', February 2019 [FFG.1020.0001.0108].

RI Advice letter to ASIC dated 4 October 2019 [FFG.1015.0003.0002].

F.4 Inadequacy of November 2019 Cybersecurity Documentation and Controls

103 As at 1 November 2019, the Cybersecurity Documentation and Controls that RI Advice held or had access to for the management of risk in respect of cybersecurity and cyber resilience across its AR network were as follows:

(a) the May 2018 Documentation and Controls referred to in paragraph 57(r) above;

(b) the IOOF Developed Documentation;

Particulars

The IOOF Developed Documentation which RI Advice held or had access to as at 1 November 2019 is set out in Schedule C.

(c) the March 2019 Documentation and Controls documents referred to in paragraphs 89(c) and (e) to (i) above;

(d) Cyber Security Standard (Version 1.0), Final Draft, dated 10 October 2019 [FFG.1022.0001.0246], which:

(i) had not been finalised, approved or released and remained a draft; and

(ii) had not been implemented across RI Advice and its ARs;

Particulars

There is no approval or release date in the document.

(e) RI Advice Information Security Policies dated 13 May 2019 [FFG.1026.0001.0101], which:

(i) had not been finalised, approved or released; and

(ii) had not been implemented across RI Advice and its ARs;

Particulars

The document contains yellow highlights and references to 'XXXX", is not signed, and was not referred to in RI Advice's letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003].

(f) RI Advice Cyber Security Support Guide dated about May 2019 [RIF.0006.0001.0001];

(g) Cybersecurity Incident Response Plan – Data Breach Process Guide dated 8 May 2019 (Version 1.0) [FFG.1020.0001.0133] and RI Advice

Cybersecurity Incident Response Plan Process Guide (CIRP) Process Guide: Data Breach (Version 1.1) dated 25 June 2019, which:

(i) were in draft form and had not been finalised, approved or released; and

(ii) had not been implemented across RI Advice and its ARs;

Particulars

The RI Advice Cybersecurity Incident Response Plan Process Guide (CIRP) Process Guide: Data Breach (Version 1.3) dated 22 April 2020 [RIF.0006.0011.0001] refers to the earlier version (version 1.0) dated 8 May 2019 as a "First Draft" and another version (version 1.1) of this document dated 25 June 2019.

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003], items 3 and 6(k).

(h) an RI Advice software asset register (spreadsheet) dated about 31 October 2019 [FFG.1022.0001.1154];

(i) guidance, questionnaires, checklists and audits in respect of implementation of password management and two factor authentication;

Particulars

Cyber Security Attestation - First collector (1) questionnaire dated about 9 October 2019 [FFG.1022.0001.3514].

AR Responses (13) to questions on implementation on password management and two factor authentication [spreadsheet] dated about 9 October 2019 [FFG.1022.0001.3521].

How to Password Protect RI Advice Adobe PDF Documents dated 9 October 2019 [FFG.1022.0001.1542].

Password Management and 2FA dated about 1 November 2019 [FFG.1022.0001.3518];

Sophos XG Firewall dated 1 November 2019 [FFG.1022.0001.3483].

How to Turn on 2FA for Adobe dated 1 November 2019 [FFG.1022.0001.3476].

How to Turn on 2FA for Google dated 1 November 2019 [FFG.1022.0001.1561].

How to Turn on 2FA for Microsoft dated 1 November 2019 [FFG.1022.0001.3509].

RI Advice Setting up Two-Factor Identification dated 1 November 2019 [FFG.1022.0001.3480].

Review of AR use of multifactor authentication in XPLAN 2019-06-12-2FA [spreadsheet] dated 1 November 2019 [FFG.1022.0001.3475].

Lastpass audit report dated 27 September 2019 [RIF.0006.0014.0003].

Cyber Security RI Mandatory Requirements Checklist dated 29 October 2019 [FFG.1022.0001.0421].

(j) PSA Completed Report [spreadsheet] dated 1 November 2019 [FFG.1022.0001.3522];

(k) PSA Review Guide Blank (1) [spreadsheet] dated 1 October 2019 [FFG.1022.0001.3523];

(l) presentations, webinars and newsletters covering cybersecurity awareness related topics; and

Particulars

It All Started with An Email Presented by Michael Connory, CEO dated 10 October 2019 [FFG.1022.0001.2825].

RI Report 23 April 2019 [FFG.1022.0001.2766].

RI Report 29 April 2019 [FFG.1022.0001.2803].

RI Report 6 May 2019 [FFG.1022.0001.2816].

RI Report 13 May 2019 [FFG.1022.0001.2659].

RI Report 20 May 2019 [FFG.1022.0001.2760].

RI Report 27 May 2019 [FFG.1022.0001.2785].

RI Report 3 June 2019 [FFG.1022.0001.2791].

RI Report 17 June 2019 [FFG.1022.0001.2749].

RI Report 22 July 2019 [FFG.1022.0001.2680].

RI Report 24 June 2019 [FFG.1022.0001.2772].

RI Report 1 July 2019 [FFG.1022.0001.2724].

RI Report 29 July 2019 [FFG.1022.0001.2695].

RI Report 5 August 2019 [FFG.1022.0001.2716].

RI Report 12 August 2019 [FFG.1022.0001.2650].

RI Report 19 August 2019 [FFG.1022.0001.2673; RIF.0006.0012.0043].

Cybersecurity Kaplan questions dated about 10 October 2019 [FFG.1022.0001.2561].

Review of Cyber Security Completion [spreadsheet] dated 1 November 2019 [FFG.1022.0001.3474].

Webinar links dated 10 October 2019 [FFG.1020.0001.0425].

(m) RI Advice procedures, application forms and checklists for recruitment, appointment and cancellation of ARs and RI Advice Practices; and

Particulars

The documents referred to in paragraphs 57(q) and 89(d) above (with the exception of the ADG Recruitment Fact Find (Version 15) dated February 2018 [FFG.1022.0001.2377]; RI Advice Authorised Representative Application Form, Version 18, April 2018 [FFG.1022.0001.1679]; RI Advice Practice Application Form Version 14, May 2017 [FFG.1022.0001.1702]); and RI Advice APPOINTMENT: Authorised Representative Appointment Checklist dated about 6 February 2016 [FFG.1022.0001.1654].

TERMINATION: AR & CAR Cancellation Checklist dated about 31 October 2019 [FFG.1022.0001.1843].

(n) CARR reports and reports in respect of Cybersecurity Incidents;

Particulars

The CARR reports referred to in paragraphs 78 and 102(a) above and the particulars thereto.

Email from Kylie Weatherall, Empowered, to Wen Li Zhou, Incident Manager, IOOF dated 3 September 2019 attaching file note from Kevin Treacey of Kevcom [FFG.1029.0001.0032, FFG.1029.0001.0035].

(the **November 2019 Documentation and Controls**).

104 As at 1 November 2019, RI Advice did not have in place any Cybersecurity Documentation and Controls for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 103 above.

105 By its November 2019 Documentation and Controls, as at 1 November 2019, RI Advice:

(a) did not adequately document the roles and responsibilities of RI Advice and its ARs as to the management of risk in respect of cybersecurity and cyber resilience across its AR network;

(b) predominantly relied upon the IOOF Developed Documentation, which:

(i) in many cases pre-dated IOOF's acquisition of RI Advice;

(ii) was specific to the IOOF organisation and its IT environment;

(iii) was not tailored to RI Advice and its ARs' requirements for the management of risk in respect of cybersecurity and cyber resilience across its AR network; and

(iv) had not been implemented and operationalised by RI Advice as part of, alternatively was not relevant to, its governance and management of risk in respect of cybersecurity and cyber resilience across its AR network.

Particulars

The IOOF Developed Documentation which RI Advice held or had access to as at 1 November 2019 which had the characteristics referred to in sub-paragraphs (i) to (iv) above is set out in Schedule C.

(c) did not adopt and implement adequate Cybersecurity Documentation and Controls in each of the 13 Cybersecurity Domains;

(d) did not meet the Minimum Cybersecurity Requirements; and

(e) did not adequately manage risk in respect of cybersecurity and cyber resilience across its AR network.

Particulars

In respect of sub-paragraphs (a), (c), (d) and (e) above, the gaps between the November 2019 Documentation and Controls and the Cybersecurity Documentation and Controls which RI Advice should have had in place in each of the 13 Cybersecurity Domains in order to meet the Minimum Cybersecurity Requirements are set out in Schedule E.

RI Advice was required to have Cybersecurity Documentation and Controls in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network. The obligation was upon RI Advice.

The Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum Cybersecurity Requirements should have adequately addressed each of the 13 Cybersecurity Domains by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

RI Advice should have had each of the Cybersecurity Documentation and Controls specified in Schedules A and E in place in each of the 13 Cybersecurity Domains prior to and as 1 November 2019 in order to meet the Minimum Cybersecurity Requirements by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 to 15 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

F.5 Contraventions in respect of conduct up to, or as at, 1 November 2019

106 By reason of the matters pleaded in paragraphs 2 to 5, 11 to 15, 85 to 91 and 100 to 105 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72 ~~and~~, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above, at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and

knowledge of the other matters pleaded in paragraphs 67 to 84 above; and/or

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 50 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that the public is entitled to expect, at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance

measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above; and/or

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and

knowledge of the other matters pleaded in paragraphs 73 to 80 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws are detailed in paragraphs 13 to 15 above and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 106(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 106(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 106(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 106(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant resources in respect of cybersecurity and

cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk;

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times from 13 March were the March 2019 Documentation and Controls, and on 1 November 2019, were the November Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience from 13 March 2019, comprising the March 2019 Documentation and Controls and as at 1 November 2019, comprising the November 2019 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above; and/or

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the

respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, exposed the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times from 13 March were the March 2019 Documentation and Controls, and on 1 November 2019, were the November Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act at all times from 13 March to 1 November 2019, alternatively on 1 November 2019, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience comprising from 13 March 2019, the March 2019 Documentation and Controls and as at 1 November 2019, the November 2019 Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above; and/or

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times from 13 March to 1

November 2019, alternatively on 1 November 2019, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

(f) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (a), (d) and (e) above, contravened s 912A(5A) of the Act.

F.6 Contraventions in respect of FFG Data Breach

106A Further to paragraph 106 above, by reason of the matters pleaded in paragraphs 2 to 5, 11 to 15, 98 and 99 above, at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, by reason of the conduct pleaded in paragraph 99 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 98 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, at

all times since 30 September or 1 November 2019, alternatively on 1 November 2019, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that the public is entitled to expect, at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, by reason of the conduct pleaded in paragraph 99 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 98 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the

financial services laws are detailed in paragraphs 13 to 15 above and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 106A(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 106A(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 106A(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 106A(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience were as at 13 March 2019, the March 2019 Documentation and Controls, from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising as at 13 March 2019, the March 2019 Documentation and Controls, from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 99 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 98 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, exposed the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk.

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience were as at 13 March 2019, the March 2019 Documentation and Controls, from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising as at 13 March 2019, the March 2019 Documentation and Controls, from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 99 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 98 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

G. INADEQUACY OF STEPS TAKEN BY RI ADVICE UP TO 1 MAY 2020 AND INADEQUACY OF CYBERSECURITY SYSTEMS IN PLACE AS AT 1 MAY 2020

G.1 Inadequacy of steps taken by RI Advice in respect of Empowered Cybersecurity Incident

107 By 18 November 2019 at the latest, RI Advice:

(a) was aware, or ought to have become aware, in respect of the Empowered Cybersecurity Incident, that it had been reported that:

(i) an external IT service provider had investigated the incident and ascertained that:

(A) an unauthorised party had compromised an Empowered staff member's mailbox account, which had been used to send Empowered's Retail Clients and its information technology service provider phishing emails regarding a purported 'Business Proposal from Empowered Financial Partners' which requested recipients to click on a link to Dropbox (**Phishing Email**);

(B) the Phishing Email would have been sent to 174 email addresses;

(C) the unauthorised party had set up new rules in the Empowered staff member's email mailbox automatically directing all incoming emails to an RSS feed email folder so that their incoming emails would not appear in the email inbox;

(D) in the Dropbox cloud file storage account there was a 'OneDrive document' that was 'capturing credentials' of people who tried to access it by clicking on the link in the Phishing Email, which file was shared with the entire contents of the Empowered staff member's email contact list and the list was able to be exported;

(E) some recipients of the Phishing Email may have clicked on the link and opened the fie in Dropbox before it was removed from Dropbox by the external IT service provider; and

(F) the unauthorised party possibly had access to the Empowered staff member's Microsoft Office 365 email mailbox 'for days' and the third party may have had a 'copy of the contents' of the Empowered staff member's 'entire email'; and

(ii) the external IT service provider had determined that the root cause of the incident was a suspected phishing email that had been received the week before;

(b) had endorsed or allowed the Empowered Cybersecurity Incident to be recorded in the Aligned Dealer Group Incident Register and the incident had been endorsed by the RI Advice Event Working Group for closure in the Aligned Dealer Group Incident Register, or ought to have become aware that this had occurred; and

(c) recorded, or ought to have become aware that it had been recorded, that the remediation and follow up steps undertaken by Empowered and RI Advice in respect of the Empowered Cybersecurity Incident, prior to the incident being endorsed for closure in the Aligned Dealer Group Incident Register, were limited to the following:

(i) Empowered had contacted its external information technology technician, who had removed the 'OneDrive document' from Dropbox and/or the 'virus' and provided a list of names of the 174 email addresses to which it considered that the Phishing Email would have been sent, and Empowered had sent an email to those contacts alerting them to the virus;

(ii) the external information technology technician had reset the password of the compromised mailbox, reset the password of the Dropbox cloud file storage account, and disabled the mailbox

ruleset in the compromised mailbox (so that incoming emails would no longer be automatically placed in the RSS feed folder);

(iii) the IOOF Head of Cybersecurity had been informed of the incident and had been provided with a report from the external information technology technician;

(iv) the IOOF Head of Cybersecurity had advised RI Advice that no further IT related actions, including any secondary IT review, were necessary, although a dedicated cybersecurity training session for all staff would be helpful, which training the IOOF IT Security team could provide;

(v) Empowered had confirmed that the compromised data comprised only names and email addresses;

(vi) the RI Advice Event Working Group forum noted that a training session would be provided to staff when the 'new standard' was released; and

(vii) RI Advice had received advice that the incident was not a notifiable data breach and that the incident had been handled correctly.

Particulars

The various reported matters and steps taken in respect of the Empowered Cybersecurity incident referred to in sub-paragraphs (a) to (c) above were recorded in the following documents:

Incident Case Record Timeline for incident IFR-02188 [FFG.1029.0001.0026].

Email from Jeannette McShane, RI Advice to IOOF Advice Risk, re Incident – Cyber Breach dated 23 August 2019, forwarded by Wen Li Zhou, Incident Manager at IOOF to Peter Ornsby and others [FFG.1029.0001.0028].

Email from Kylie Weatherall, Empowered, to Wen Li Zhou, Incident Manager, IOOF dated 3 September 2019 attaching file note from

Kevin Treacey of Kevcom [FFG.1029.0001.0032, FFG.1029.0001.0035].

Email chain between Ashutosh Kapse, Head of Cybersecurity, IOOF, and Wen Li Zhou between 26 August 2019 and 30 September 2019 [FFG.1029.0001.0036].

Email from Jeannette McShane, RI Advice to Peter Ornsby, dated 16 October 2019 [FFG.1029.0001.0043].

Further, as to RI Advice's knowledge of the matters referred to in sub-paragraphs (a) to (c) above, the plaintiff refers to and repeats paragraph 16 above.

108 By reason of the matters pleaded in paragraphs 2(d) and (e), 3 to 5, 11 to 15, 94, 95 and 107 above, and with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 63 and 64(a), 81 to 84, 96 and 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above, after becoming aware, or after it ought to have become aware, of the Empowered Cybersecurity Incident and prior to endorsing the close out of the Empowered Cybersecurity Incident in the Aligned Dealer Group Incident Register, RI Advice should have:

(a) identified gaps or deficiencies within the Cybersecurity Documentation and Controls relevant to the root cause of the Empowered Cybersecurity Incident referred to in paragraph 107(a)(ii) above; and

(b) incorporated the findings about the root cause and lessons learnt from the Empowered Cybersecurity Incident into its ongoing identification and mitigation of risk in respect of cybersecurity and cyber resilience across its AR network, by:

(i) undertaking a cybersecurity and cyber resilience risk assessment across its entire AR network, and seeking Technical Security Assurance across a number of its ARs, of the effectiveness of the following Cybersecurity Documentation and Controls relevant to the Empowered Cybersecurity Incident;

(A) Cyber training and awareness;

(B) Multi-factor authentication;

(C) Incident response; and

(D) Email filtering;

Particulars

Details of the following relevant Cybersecurity Documentation and Controls are provided in Schedule A:

(a) Cyber training and awareness [ED 6.1 to ED 6.7];

(b) Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6];

(c) Incident response [ED 12.1 to ED 12.5]; and

(d) Email filtering [ED 9.4 to ED 9.8].

(ii) based on an analysis of this information, determining the current cybersecurity risks applicable to its AR network; and

(iii) developing and implementing a cybersecurity remediation plan for the Empowered Cybersecurity Incident which was tailored to the identified cybersecurity risks applicable to its AR network, including promptly reviewing and remediating any gaps or deficiencies in its Cybersecurity Documentation and Controls.

Particulars

In respect of the Empowered Cybersecurity Incident, RI Advice should have taken the steps pleaded in paragraphs 108(a) and (b) above by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the facts, matters and circumstances pleaded in paragraphs 13 to 15, 94, 95 and 107 above, and with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 63 and 64(a), 81 to 84, 96 and 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above,

and at trial ASIC will rely on the Bell Report.

109 RI Advice did not take the steps referred to in paragraph 108 above, adequately or at all, by 18 November 2019 or at any relevant time.

Particulars

The only steps taken were those set out in paragraph 107(c) above, which did not amount to taking the steps referred to in paragraph 108 above adequately or at all.

G.2 Contraventions in respect of Empowered Cybersecurity Incident

110 By reason of the matters pleaded in paragraphs 2 to 5, 11 to 15, 94, 95 and 107 to 109 above, at all times since 18 November 2019, RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act at all times since 18 November 2019, by reason of the conduct pleaded in paragraph 109 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 94, 95, 107 and 108 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, at all times since 18 November 2019, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that the public is entitled to expect, at all times since 18 November 2019, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act at all times since 18 November 2019, by reason of the conduct pleaded in paragraph 109 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 94, 95, 107 and 108 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws are detailed in paragraphs 13 to 15 above and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 110(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 110(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 110(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 110(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk;

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience were at all times since 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act at all times since 18 November 2019, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 109 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 94, 95, 107 and 108 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times since 18 November 2019, exposed the

persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience since 1 November 2019 were the November 2019 Documentation and Controls, and as at 1 May 2020, were the May 2020 Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act at all times since 18 November 2019, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of the conduct pleaded in paragraph 109 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 94, 95, 107 and 108 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times since 18 November 2019, were inadequate to prevent the exposure of the persons to

whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

(f) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (a), (d) and (e) above, contravened s 912A(5A) of the Act.

G.3 Second RI Shepparton Cybersecurity Incident – April 2020

111 On or about 15 April 2020, RI Advice became aware of a Cybersecurity Incident that occurred on about 14 April 2020 involving Sandra Miller and RI Shepparton (**Second RI Shepparton Cybersecurity Incident**).

Particulars

Incident report submission lodged by RI Shepparton with RI Advice Risk Team dated 15 April 2020 [RIF.0006.0016.0001].

Letter from RI Advice to RI Shepparton dated 20 April 2020 attaching completed incident report (IFR-02797) [FFG.1029.0001.0020].

Letter from RI Advice to ASIC dated 1 May 2020 in response to Notice issued by ASIC under s 912C of ASIC Act (Reference 18-20364) [FFG.1027.0001.0003 at .0011].

112 By about 1 May 2020 at the latest, RI Advice:

(a) was aware, in respect of the Second RI Shepparton Cybersecurity Incident, that it was reported that:

(i) like the First RI Shepparton Cybersecurity Incident, it involved an external party's unauthorised use of Sandra Miller's RI Shepparton email account;

(ii) as a consequence, spam emails were sent from Sandra Miller's email account to her RI Advice and IOOF contacts, fund managers, and five Retail Clients in her email contacts (**Spam Emails**); and

(iii) a third-party information technology service provider had reviewed the incident and had concluded that the external party had obtained access to Sandra Miller's email account, possibly through a Microsoft Office log-in, at some time in the last five years and had only just now used it;

(b) recorded that the remediation and follow up steps undertaken by RI Shepparton and RI Advice in respect of the Second RI Shepparton Cybersecurity Incident were limited to the following:

(i) a third-party information technology service provider had removed global administration rights from Sandra Miller's RI Shepparton email account and had ensured that there were no global or user level forwarding rules which had been created from the account;

(ii) RI Shepparton had reported that it had sent an email to all recipients to tell them not to open the Spam Emails; all outgoing emails from the affected email account had ceased within one hour after the incident; all 'LastPass' password manager passwords had been changed on or about 14 April 2020; and two-factor authentication had been employed on 'all client systems', which RI Shepparton reported was 'already in place';

(iii) RI Advice had notified the IOOF Privacy Officer and IOOF Fraud team seeking guidance about any steps which RI Shepparton should take in addition to the steps that had already been undertaken by RI Shepparton; and RI Advice had requested RI Shepparton to refer to the IOOF Privacy Officer and the IOOF Fraud team and complete RI Shepparton's remediation by 11 May 2020; and

(iv) RI Advice had engaged Security in Depth to perform a review of the Second RI Shepparton Cybersecurity Incident to identify the root cause of the incident, which report was expected after 4 May 2020.

Particulars

Email from DWM Support to RI Shepparton, forwarded to RI Advice dated 14 April 2020 [FFG.1029.0001.0018].

Incident report submission lodged by RI Shepparton with RI Advice Risk Team dated 15 April 2020 [RIF.0006.0016.0001].

Letter from RI Advice to RI Shepparton dated 20 April 2020 attaching completed incident report (IFR-02797) [FFG.1029.0001.0020].

Letter from RI Advice to ASIC dated 1 May 2020 in response to Notice issued by ASIC under s 912C of ASIC Act (Reference 18-20364) [FFG.1027.0001.0003 at .0011].

113 On or about 19 May 2020, after performing a review and assessment of RI Shepparton, Security in Depth provided RI Advice with a CARR report in respect of RI Shepparton dated April 2020, which:

(a) rated RI Shepparton's cybersecurity status as still 'Poor' (page 3);

(b) identified that the cause of the Second RI Shepparton Cybersecurity 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 (page 3); and

(c) referred to a number of 'significant cybersecurity issues', including:

(i) the poor level of password security across RI Shepparton (page 3);

(ii) no utilisation of two factor authentication (page 3);

(iii) that RI Shepparton's current infrastructure settings would allow a sophisticated threat actor to access the current network and email infrastructure which incorporated significant personally identifiable information (page 3);

(iv) that RI Shepparton had not effectively reviewed and understood the critical assets they manage and had not identified strategies to protect and maintain them (page 5);

(v) that RI Shepparton had not utilised security technologies across the organisation to identify the occurrence of a cyber security incident (page 7); and

(vi) that RI Shepparton did not have an incident response plan or a fully-developed business continuity plan (page 8 and 9).

Particulars

Cyber Assurance Risk Rating Report– RI Advice - Shepparton [FFG.1029.0001.0006].

114 But for RI Advice's failures to take the steps referred to in paragraph 65 above and its contraventions referred to in paragraphs 92 and 106 above, the Second Shepparton Cybersecurity Incident may not have occurred.

Particulars

Both the First Shepparton Cybersecurity Incident and the Second Shepparton Cybersecurity Incident involved the compromise of an AR's email account. But for RI Advice's failure to adequately remediate the gaps and deficiencies in the Cybersecurity Documentation and Controls relevant to the First Shepparton Cybersecurity Incident across its AR network (including the Cyber training and awareness [ED 6.1 to ED 6.7], Email filtering [ED 9.4 and ED 9.8] and Multi-factor authentication [ED 5.1, ED 5.3 and ED 5.6] controls) by 12 March 2019, alternatively 1 November 2019, the Second Shepparton Cybersecurity Incident was unlikely to have occurred.

G.4 Inadequacy of steps taken by RI Advice up to 1 May 2020

115 By 1 May 2020, RI Advice had planned and/or undertaken the following cybersecurity initiatives to address cybersecurity issues across its AR network

and to prevent and manage Cybersecurity Incidents (**May 2020 Cybersecurity Initiatives**):

(a) Six CARRs;

(b) Cybersecurity Discussion Topics;

(c) Documentation Update;

(d) Attestations on Cyber Capabilities and Protections;

(e) Awareness Material;

(f) Mandated MFA;

(g) Mandated Password Management;

(h) Cybersecurity Leadership;

(i) Gap Analysis;

(j) Review of Cyber Standard;

(k) Cybersecurity Incident Response Plan Finalisation;

(l) Training Implementation;

(m) Cyber Insurance;

(n) initiation of a cybersecurity strategy (**Cybersecurity Strategy**); and

(o) establishment of the Advice Processes and Client Records program, which would require ARs to store all Personal Information in the Xplan database (**ACR Program**).

Particulars

RI Advice letter to ASIC dated 25 January 2019 [FFG.1013.0001.0003].

RI Advice letter to ASIC dated 30 January 2019 [FFG.1014.0001.0062].

RI Advice letter to ASIC dated 4 October 2019 [FFG.1015.0003.0002].

RI Advice letter to ASIC dated 1 November 2019 [FFG.1021.0001.0003].

RI Advice letter to ASIC dated 28 November 2019 [FFG.1023.0001.0003].

RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003].

Further particulars of the matters pleaded in sub-paragraphs (a) to (o) above are provided in paragraph 117 below.

116 As at 1 May 2020, RI Advice had not planned or implemented any initiatives for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 115 above.

117 As at 1 May 2020, RI Advice had only implemented the May 2020 Cybersecurity Initiatives to the extent referred to below:

(a) the Six CARRs were complete;

(b) the Cybersecurity Discussion Topics had been implemented at the PAC and the RI Event Working Group;

(c) the Documentation Update was complete, and RI Advice:

(i) had developed the Cybersecurity Documents and Controls referred to in paragraphs102(c)(iii) to (v) and 103(f) above and 118(d) and (f) below;

(ii) but was developing the RI Advice Information Security Policies referred to in paragraph 118(c) below, which had not been finalised, approved or released;

(d) in respect of the Attestations on Cyber Capabilities and Protections:

(i) the updated Cyber Security Guide [RIF.0006.0001.0001] referred to in paragraph 118(f) below was provided to ARs on 2 December 2019;

(ii) only 34 of 89 RI Advice Practices had provided attestation to the adoption of the 11 'best practice' cybersecurity elements referred to in paragraph 118(f) below; and

(iii) a final due date for this to be completed had not been set;

Particulars

On 20 April 2020, RI Advice requested ARs to provide attestation from the technical support executive from each RI Advice Practice to the adoption of the 11 elements in the Cyber Security Guide and had received attestations from 34 of 89 RI Advice Practices [RIF.0006.0013.0001]. RI Advice was following up with RI Advice Practices who had not attested to full implementation, but no date was set for completion: RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], items 1(a) and 6.

(e) Awareness Material had continued but had not been completed;

Particulars

As at 1 November 2019, RI Advice had recorded that 110 ARs had completed the 'Cyber Fraud' or 'Cyber Security Training Essentials' training sessions between about 2 May and 20 August 2019 and 88 ARs had not yet completed this training [FFG.1022.0001.3474].

During November and December 2019, RI Advice conducted a series of Cyber Security presentations to the AR network, and between February and May 2020, RI Advice, supported by Security in Depth, conducted two webinars (Part A and Part B) for its adviser network to raise awareness about the management of cyber security risks relevant to their practices: RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], items 1(a) and (d).

121 ARs or support staff attended the cybersecurity Part A webinar, and 128 attended the Part B webinars hosted by Security in Depth [RIF.0006.0004.0001].

(f) Draft cyber security standard questions relating to the cyber awareness material had yet to be developed.in respect of Mandated MFA, RI Advice had received attestations from its ARs that they had implemented multifactor authentication in Xplan;

Particulars

RI Advice had received attestations from all RI Advice Practices that they had two factor authentication in place in respect of Xplan. RI Advice monitored compliance with the 2FA requirements of Xplan since 4 October 2019 by reviewing monthly on-line audit reports: RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], items 1(f) and 4.

All_Users_2FA__RI JAN dated 17 January 2020 [RIF.0006.0006.0007].

16 December 2019 Outstanding Xplan 2FA (spreadsheet) dated about 16 December 2019 [RIF.0006.0006.0001].

20 November 2019 Outstanding Xplan 2FA (spreadsheet) dated about 20 November 2019 [RIF.0006.0006.0002].

21042020 2FA Report dated about 21 April 2020 spreadsheet [RIF.0006.0006.0003] which recorded that 96% of users had activated two factor authentication in Xplan.

2019-06-12-2FA spreadsheet dated about June 2019 [FFG.1022.0001.3475].

As alleged in paragraph 113(c)(ii) above, Security in Depth reported in its April 2020 CARR that RI Shepparton had no utilisation of two factor authentication.

(g) Mandated Password Management was complete;

Particulars

LastPass, which was not a mandatory password management system, had been implemented by 215 ARs and practice staff (approximately 42% of users).

RI Advice reviewed on-line audit reports available from the LastPass system about the implementation of Lastpass: LastPass audit reports: [RIF.0006.0014.0005 (17 April 2020), RIF.0006.0014.0002 (22 April 2020) and RIF.0006.0014.0003 (27 April 2019)].

RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], item 1(f) and 7.

(h) Cybersecurity Leadership was incomplete;

Particulars

There was no development of specific roles and teams to manage cyber events (such as "Head of IT Cyber Security") across RI Advice and its ARs.

(i) the Gap Analysis was incomplete and:

(i) the scope of the Gap Analysis had been expanded so that a cyber assessment was planned to be performed on each RI Advice Practice, which was not expected to be completed until the end of 2020; and

(ii) draft cyber assessments for only 3 of the 89 RI Advice Practices had been completed, which had yet to be considered by RI Advice for any formal recommendations;

Particulars

The following three draft reports had been provided to RI Advice, which had yet to be considered by RI Advice for any formal recommendations:

Cyber Assurance Risk Rating Report Bountiful Wealth dated 23 April 2020 [RIF.0006.0010.0014];

Cyber Assurance Risk Rating Report: Benchmark Consultants dated 27 April 2020 [RIF.0006.0010.0004]; and

Cyber Assurance Risk Rating Report: RI Advice Berwick dated 27 April 2020 [RIF.0006.0010.0025].

RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], item 1(j).

(j) the Review of the Cyber Standard was incomplete and:

(i) the Cyber Security Standard was released on 30 March 2020, and ARs were expected to successfully complete a planned examination on its contents by 30 June 2020; and

(ii) no attestations or audits to verify that all ARs had fully implemented the Cyber Security Standard had been completed;

Particulars

No analysis had been conducted of the implementation of the new Cyber Standard.

The Cyber Security Standard [RIF.0006.0002.0065] was released and uploaded to the RI Intranet on 30 March 2020. It was planned that ARs would be tested on this standard as part of an exam which was planned to be available from 11 May 2020, and that ARs were to complete by 30 June 2020: RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], items 1(d) and (i).

(k) in respect of the Cybersecurity Incident Response Plan Finalisation, the Cybersecurity Incident Response Plan was released on 22 April 2020 and provided to ARs on 27 April 2020;

Particulars

RI Advice Cybersecurity Incident Response Plan Process Guide (CIRP) Process Guide: Data Breach (Version 1.3) dated 22 April 2020 [RIF.0006.0011.0001].

RI Advice provided the Cybersecurity Incident Response Plan to ARs via a link in a newsletter dated 27 April 2020 [RIF.0006.00005.0098].

RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], item 1(c).

(l) Training Implementation was incomplete although ARs were expected to successfully complete a planned examination on the webinar contents by 30 June 2020;

Particulars

No training modules relating to ISO 27001 and ASD Essential Eight policy and procedure development had been completed.

The training implemented as at 1 May 2020 is referred to in sub-paragraph (e) above.

It was planned that ARs would be tested on the content of the webinars through an exam which was planned to be available from 11 May 2020 that ARs were to complete by 30 June 2020:
RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], item 1(d).

(m) Cyber Insurance had been obtained and was being offered to ARs;

(n) RI Advice expected to have implemented the Cybersecurity Strategy by the end of 2020, but no formal documentation of the proposed strategy had been completed; and

Particulars

No relevant documentation is referred to in RI Advice's letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], item 11.

(o) RI Advice expected to have implemented the ACR Program by the end of 2020.

Particulars

The program was commenced on 19 October 2019 and RI Advice expected it to be implemented by the end of 2020: RI Advice letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003], item 1(h).

The ACR Nominations and Training Logs - RI Advice [spreadsheet] dated 27 April 2020 [RIF.0006.0008.0001] recorded that approximately 10 RI Advice Practices had attended relevant training sessions.

Advice Processes and Client Records guide dated 27 April 2020 [RIF.0006.0008.0002].

G.5 Inadequacy of May 2020 Cybersecurity Documentation and Controls

118 As at 1 May 2020, the Cybersecurity Documentation and Controls that RI Advice held or had access to for the management of risk in respect of cybersecurity and cyber resilience across its AR network were as follows:

(a) the IOOF Developed Documentation;

Particulars

The IOOF Developed Documentation which RI Advice held or had access to as at 1 May 2020 is set out in Schedule C.

(b) the November 2019 Documentation and Controls referred to in paragraph 103 above with the exception of the documents referred to in paragraphs 103(b) and (g) above;

(c) the RI Advice Information Security Policies dated 13 May 2019 [FFG.1026.0001.0101] referred to in paragraph 103(e) above, which:

(i) had not been finalised, approved or released; and

(ii) had not been implemented across RI Advice and its ARs;

Particulars

The document contains yellow highlights and references to 'XXXX", and is not signed.

The document is not referred to in RI Advice's letter to ASIC dated 1 May 2020 [FFG.1027.0001.0003].

(d) Cyber Security Standard, released on 30 March 2020 [RIF.0006.0002.0065];

(e) RI Advice Cybersecurity Incident Response Plan Process Guide (CIRP) Process Guide: Data Breach (Version 1.3) dated 22 April 2020 [RIF.0006.0011.0001];

(f) an updated version of the Cyber Security Support Guide [RIF.0006.0001.0001] dated about May 2019, which referred to the following 11 'RI Advice Group best practices':

(i) use a Firewall;

(ii) patch;

(iii) document your cybersecurity policies;

(iv) use a VPN;

(v) educate all employees;

(vi) enforce safe password practices;

(vii) regularly back up all data;

(viii) install anti-malware software;

(ix) use multifactor identification;

(x) password protection for emails and correspondence; and

(xi) prepare for a brute force attack.

(g) Security in Depth document titled 'CARR Framework Questions' dated about 23 April 2020 [RIF.0006.0010.0003];

(h) Small Business Cyber Security Guide dated 2 April 2020 [RIF.0006.0002.0189] developed by the Australian Cyber Security Centre;

(i) Electronic Data Storage (Version 1.0), effective date 1 January 2020 [FFG.1022.0001.2213];

(j) guidance, questionnaires, audits and notifications on implementation of password management and two factor authentication;

Particulars

How to Password Protect a PDF file for Free dated 27 April 2020 [RIF.0006.0002.0103].

How to Password Protect RI Advice Word Documents dated 27 April 2020 [RIF.0006.0002.0131].

LastPass FAQs dated 27 April 2020 [RIF.0006.0002.0145].

Work at Home Protection: Quick Security Tips dated 27 April 2020 [RIF.0006.0002.0139].

2FA Guide – Google dated 27 April 2020 [RIF.0006.0002.0029].

LastPass - Professional Services Enterprise Brief [USD] dated 27 April 2020 [RIF.0006.0002.0140].

LastPass Desktop Quick Reference Guide dated about 27 March 2020 [RIF.0006.0002.0143].

LastPass Enterprise Onboarding CSM dated 27 April 2020 [RIF.0006.0002.0144].

LastPass Notification: Improve your passwords! Dated 16 April 2020 [RIF.0006.0014.0001].

Lastpass report dated April 2020 [RIF.0006.0014.0002].

(k) spreadsheet recording ARs' implementation of two factor authentication;

Particulars

All_Users_2FA__RI JAN dated 17 January 2020 [RIF.0006.0006.0007].

16 December 2019 Outstanding Xplan 2FA (spreadsheet) dated about 16 December 2019 [RIF.0006.0006.0001].

20 November 2019 Outstanding Xplan 2FA (spreadsheet) dated about 20 November 2019 [RIF.0006.0006.0002].

21042020 2FA Report dated 29 April 2020 spreadsheet [RIF.0006.0006.0003].

(l) presentations, webinars and newsletters, cybersecurity questions and mandatory cybersecurity induction questions, and exam questions and attestations, and communications with ARs covering cybersecurity awareness related topics;

Particulars

Cyber Exam [spreadsheet] dated 26 April 2020 [RIF.0006.0004.0087].

Cyber Security Webinar - Presentation Link dated 6 April 2020 [RIF.0006.0002.0036].

IOOF Cyber Resilience Initiative presentation by Security in Depth dated 26 April 2020 [RIF.0006.0004.0003].

IOOF Cyber Resilience presentation by Security in Depth dated 26 April 2020 [RIF.0006.0004.0042].

Cyber Resilience - Intranet Content [screenshot] dated 27 April 2020 [RIF.0006.0002.0180].

Cyber Resilience Initiative: Your participation in the pilot group dated 1 May 2020 [RIF.0006.0010.0001].

Cyber Security CEO Update dated 30 April 2020 [RIF.0006.0001.0010].

RI Report 18 November 2019 [RIF.0006.0005.0045].

RI Report 25 November 2019 [RIF.0006.0005.0083].

RI Report 2 December 2019 [RIF.0006.0005.0052].

RI Report 9 December 2019 [RIF.0006.0005.0009].

RI Report 28 January 2020 [RIF.0006.0005.0091].

RI Report 10 February 2020 [RIF.0006.0005.0017].

RI Report 17 February 2020 [RIF.0006.0005.0038].

RI Report 24 February 2020 [RIF.0006.0005.0076].

RI Report 02 March 2020 [RIF.0006.0005.0062].

RI Report 09 March 2020 [RIF.0006.0005.0001].

RI Report 16 March 2020 [RIF.0006.0005.0031].

RI Report 23 March 2020 [RIF.0006.0005.0068].

RI Report 30 March 2020 [RIF.0006.0005.0104].

RI Report 06 April 2020 [RIF.0006.0005.0117].

RI Report 14 April 2020 [RIF.0006.0005.0024].

RI Report 27 April 2020 [RIF.0006.0005.0098].

Webinar Links [URLs] dated about 27 March 2020 (LastPass, Cybersecurity Webinar, LastPass Enterprise Training July 2019, Cybersecurity Essentials Part B Webinar) [RIF.0006.0002.0130].

Spreadsheet of attendees of cybersecurity webinars hosted by Security in Depth dated 30 April 2020 [RIF.0006.0004.0001].

Spreadsheet of attestations from RI Advice Practices regarding adoption of the 11 elements in the Cyber Security Guide [RIF.0006.0013.0001].

Email from Peter Ornsby re Comments on Policies dated 28 November 2019 [FFG.1026.0001.0099]

(m) CARR reports and reports in respect of Cybersecurity Incidents; and

Particulars

The CARR reports referred to in paragraphs 113 and 117(i) above and the particulars thereto.

(n) ACR Program documents referred to in paragraph 117(o) above;

(the **May 2020 Documentation and Controls**).

119 As at 1 May 2020, RI Advice did not have in place any Cybersecurity Documentation and Controls for the management of risk in respect of cybersecurity and cyber resilience across its AR network other than as referred to in paragraph 118 above.

120 By its May 2020 Documentation and Controls, as at 1 May 2020, RI Advice:

(a) did not adequately document the roles and responsibilities of RI Advice and its ARs as to the management of risk in respect of cybersecurity and cyber resilience across its AR network;

(b) relied in part upon the IOOF Developed Documentation, which:

(i) in many cases pre-dated IOOF's acquisition of RI Advice;

(ii) was specific to the IOOF organisation and its IT environment;

(iii) was not tailored to RI Advice and its ARs' requirements for the management of risk in respect of cybersecurity and cyber resilience across its AR network; and

(iv) had not been implemented and operationalised by RI Advice as part of, alternatively was not relevant to, its governance and management of risk in respect of cybersecurity and cyber resilience across its AR network.

Particulars

The IOOF Developed Documentation which RI Advice held or had access to as at 1 May 2020 which had the characteristics referred to in sub-paragraphs (i) to (iv) above is set out in Schedule C.

(c) did not adopt and implement adequate Cybersecurity Documentation and Controls in each of the 13 Cybersecurity Domains;

(d) did not meet the Minimum Cybersecurity Requirements; and

(e) did not adequately manage risk in respect of cybersecurity and cyber resilience across its AR network.

Particulars

In respect of sub-paragraphs (a), (c), (d) and (e) above, the gaps between the May 2020 Documentation and Controls and the Cybersecurity Documentation and Controls which RI Advice should have had in place in each of the 13 Cybersecurity Domains in order to meet the Minimum Cybersecurity Requirements are set out in Schedule F.

RI Advice was required to have Cybersecurity Documentation and Controls in place that were adequate to manage risk in respect of

cybersecurity and cyber resilience for itself and across its AR network. The obligation was upon RI Advice.

The Cybersecurity Documentation and Controls that RI Advice should have had in place in order to meet the Minimum Cybersecurity Requirements should have adequately addressed each of the 13 Cybersecurity Domains by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

RI Advice should have had each of the Cybersecurity Documentation and Controls specified in Schedules A and F in place in each of the 13 Cybersecurity Domains prior to and as at 1 May 2020 in order to meet the Minimum Cybersecurity Requirements by reason of:

(a) the facts, matters and circumstances pleaded in paragraphs 2(d) and (e) and 3 to 5 above;

(b) the obligations pleaded in paragraphs 11 and 12 above; and

(c) the matters pleaded in paragraph 13 to 15 above,

and at trial ASIC will rely on the Bell Report in relation to the content of appropriate Cybersecurity Documentation and Controls and Minimum Cybersecurity Requirements.

G.6 Contraventions in respect of conduct up to, or as at, 1 May 2020

121 Alternatively to paragraphs 93 and 106 above, and further or alternatively to paragraph 110 above, by reason of the matters pleaded in paragraphs 2 to 5, 11 to 15, 85 to 91, 100 to 105, 108, 109 and 115 to 120 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84, 95, 96, 97 and 107(a) above and knowledge of the other matters pleaded in paragraphs 73 to 80 above, at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, RI Advice:

(a) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

Particulars

RI Advice contravened s 912A(1)(a) of the Act at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39,

40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above;

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above;

(iii) the conduct pleaded in paragraph 120 above and Schedule F, in that its May 2020 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule F, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 115 to 119 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84, 95, 96, 97 and 107(a) above and knowledge of the other matters pleaded in paragraphs 73 to 80 above; and/or

(iv) the conduct pleaded in paragraph 109 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 94, 95, 107 and 108 above.

RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, by reason of the matters referred to above.

RI Advice's performance in respect of cybersecurity and cyber resilience did not meet the reasonable standard of performance that the public is entitled to expect, at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, by reason of the matters referred to above.

RI Advice contravened s 912A(1)(a) of the Act by failing to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, the financial services covered by the Licence were not provided efficiently or fairly.

(b) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

Particulars

RI Advice contravened s 912A(1)(b) of the Act at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above;

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above;

(iii) the conduct pleaded in paragraph 120 above and Schedule F, in that its May 2020 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule F, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 115 to 119 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84, 95, 96, 97 and 107(a) above and knowledge of the other matters pleaded in paragraphs 73 to 80 above; and/or

(iv) the conduct pleaded in paragraph 109 above, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15, 94, 95, 107 and 108 above.

The compliance measures that RI Advice was required to have in place in respect of cybersecurity and cyber resilience in order to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws are detailed in paragraphs 13 to 15 above and Schedule A.

(c) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

Particulars

The financial services laws which RI Advice did not comply with are ss 912A(1)(a), (b), (d) and (h) of the Act.

RI Advice contravened s 912A(1)(c) of the Act, by reason of:

(i) in respect of s 912A(1)(a) of the Act, the matters pleaded in paragraph 121(a) above;

(ii) in respect of s 912A(1)(b) of the Act, the matters pleaded in paragraph 121(b) above;

(iii) in respect of s 912A(1)(d) of the Act, the matters pleaded in paragraph 121(d) below; and

(iv) in respect of s 912A(1)(h) of the Act, the matters pleaded in paragraph 121(e) below.

(d) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that by reason of RI Advice's

failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant resources in respect of cybersecurity and cyber resilience:

(A) from 13 March 2019, comprised the March 2019 Documentation and Controls;

(B) from 1 November 2019, comprised the November 2019 Documentation and Controls; and

(C) on 1 May 2020, comprised the May 2020 Documentation and Controls.

RI Advice contravened s 912A(1)(d) of the Act at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising as at 13 March 2019, the March 2019 Documentation and Controls, from 1 November 2019, the November 2019 Documentation and Controls, and as at 1 May 2020, the May 2020 Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5,

13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above;

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above; and/or

(iii) the conduct pleaded in paragraph 120 above and Schedule F, in that its May 2020 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule F, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 115 to 119 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84, 95, 96, 97 and 107(a) above and knowledge of the other matters pleaded in paragraphs 73 to 80 above.

RI Advice failed to have available adequate resources (including financial, technological and human resources) to provide the

financial services covered by the Licence by reason of the matters referred to above.

RI Advice's relevant resources in respect of cybersecurity and cyber resilience at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, exposed the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

It is not alleged that RI Advice did not carry out supervisory arrangements.

(e) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that by reason of RI Advice's failures to comply with its obligations referred to in paragraphs 13 to 15 above, RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk; and

Particulars

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience:

(A) from 13 March 2019, comprised the March 2019 Documentation and Controls;

(B) from 1 November 2019, comprised the November 2019 Documentation and Controls; and

(C) on 1 May 2020, comprised the May 2020 Documentation and Controls.

RI Advice contravened s 912A(1)(h) of the Act at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, in that RI Advice's relevant risk

management systems in respect of cybersecurity and cyber resilience comprising the March 2019 Documentation and Controls, the November 2019 Documentation and Controls and the May 2020 Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk, by reason of:

(i) the conduct pleaded in paragraph 91 above and Schedule D, in that its March 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule D, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 85 to 90 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63 and 64(a) above and knowledge of the other matters pleaded in paragraphs 67 to 84 above;

(ii) the conduct pleaded in paragraph 105 above and Schedule E, in that its November 2019 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule E, in the circumstances of the facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 100 to 104 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84 and 96 to 97 above and knowledge of the other matters pleaded in paragraphs 73 to 80 above; and/or

(iii) the conduct pleaded in paragraph 120 above and Schedule F, in that its May 2020 Documentation and Controls did not meet the Minimum Cybersecurity Requirements in the respects set out in Schedule F, in the circumstances of the

facts and matters pleaded in paragraphs 2(d) and (e), 3 to 5, 13 to 15 and 115 to 119 above, including with knowledge of the matters in respect of the Cybersecurity Incidents pleaded in paragraphs 19, 20(a), 23, 24(a), 29, 30(a), 34, 35(a), 39, 40(a), 44, 45(a), 46, 48, 56, 63, 64(a), 67 to 72, 81 to 84, 95, 96, 97 and 107(a) above and knowledge of the other matters pleaded in paragraphs 73 to 80 above.

RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience at all times from 13 March 2019 to 1 May 2020, alternatively at all times since 13 March 2019, alternatively on 1 May 2020, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk by reason of the matters referred to above.

(f) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (a), (d) and (e) above, contravened s 912A(5A) of the Act.

H. RELIEF

By reason of the matters referred to above, ASIC seeks the relief stated below.

Declarations

1 Declarations that RI Advice:

(a) contravened ss 912A(1)(a), (b), (c), (d) and (h) of the Act at all times from 15 May 2018 to 12 March 2019; and

(b) contravened ss 912A(1)(a), (b), (c), (d) and (h) and (5A) of the Act at all times from 13 March 2019 to:

1) the date of judgment; alternatively

2) 1 May 2020; alternatively

3) 1 November 2019,

as a result of its failure to have strategies, frameworks, policies, plans, procedures, standards, guidelines, systems, resources and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network, and as a result of this conduct, it:

(i) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

(ii) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

(iii) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

(iv) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence

without exposing the persons to whom the financial services were supplied to an unacceptable level of risk;

(v) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk; and

(vi) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (b)(i), (iv) and (v) above, contravened s 912A(5A) of the Act.

2 Alternatively to paragraph 1 above, declarations that RI Advice:

(a) contravened ss 912A(1)(a), (b), (c), (d) and (h) of the Act on:

1) 15 May 2018; and/or

2) 12 March 2019; and/or

(b) contravened ss 912A(1)(a), (b), (c), (d) and (h) and (5A) of the Act on:

1) 13 March 2019; and/or

2) 1 November 2019; and/or

3) 1 May 2020,

as a result of its failure to have strategies, frameworks, policies, plans, procedures, standards, guidelines, systems, resources and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network, and as a result of this conduct, it:

(i) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that the

financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

(ii) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

(iii) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

(iv) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk;

(v) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons

to whom the financial services were supplied to an unacceptable level of risk; and

(vi) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (b)(i), (iv) and (v) above, contravened s 912A(5A) of the Act.

2A Further or alternatively to paragraphs 1 and 2 above, declarations that at all times since 30 September or 1 November 2019, alternatively on 1 November 2019, after becoming aware of the FFG Data Breach, RI Advice failed to take adequate steps to remediate any gaps or deficiencies across its AR network relevant to the root cause of the FFG Data Breach, and as a result of this conduct, it:

(i) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that the financial services covered by the Licence were not provided efficiently or fairly because RI's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

(ii) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

(iii) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

(iv) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk; and

(v) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk.

3 Further or alternatively to paragraphs 1, 2 and 2A above, declarations that at all times since 18 November 2019 after becoming aware of the Empowered Cybersecurity Incident, RI Advice failed to take adequate steps to remediate any gaps or deficiencies across its AR network relevant to the root cause of the Empowered Cybersecurity Incident, and as a result of this conduct, it:

(i) in contravention of s 912A(1)(a) of the Act, failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, in that the financial services covered by the Licence were not provided efficiently or fairly because RI Advice's performance in respect of cybersecurity and cyber resilience was inadequate and exposed the persons to whom the financial services were supplied to an unacceptable level of risk, and did not meet the reasonable standard of performance that the public is entitled to expect;

(ii) in contravention of s 912A(1)(b) of the Act, failed to comply with the condition of the Licence requiring it to establish and maintain compliance measures that ensure, as far as is reasonably practicable, that it complies with the provisions of the financial services laws (which relevantly comprise ss 912A(1)(a), (d) and (h) of the Act), in that RI Advice failed to establish and maintain such compliance measures in respect of cybersecurity and cyber resilience;

(iii) in contravention of s 912A(1)(c) of the Act, failed to comply with the financial services laws (which relevantly comprise ss 912A(1)(a), (b), (d) and (h) of the Act);

(iv) in contravention of s 912A(1)(d) of the Act, failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, in that RI Advice's relevant resources in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to provide the financial services covered by the Licence without exposing the persons to whom the financial services were supplied to an unacceptable level of risk;

(v) in contravention of s 912A(1)(h) of the Act, failed to have adequate risk management systems, in that RI Advice's relevant risk management systems in respect of cybersecurity and cyber resilience, comprising its Cybersecurity Documentation and Controls, were inadequate to prevent the exposure of the persons to whom the financial services were supplied to an unacceptable level of risk; and

(vi) by reason of the contraventions of each of ss 912A(1)(a), (d) and (h) of the Act referred to in sub-paragraphs (b)(i), (iv) and (v) above, contravened s 912A(5A) of the Act.

Pecuniary penalties

4 RI Advice pay pecuniary penalties in relation to each of the contraventions of s 912A(5A) of the Corporations Act referred to in paragraphs 1(b)(vi), alternatively 2(b)(vi), and, further or alternatively, 3(vi) above.

Compliance orders

5 RI Advice must, within 3 months of the date of these Orders, have strategies, frameworks, policies, plans, procedures, standards, guidelines, systems, resources and controls in respect of cybersecurity and cyber resilience in place that are adequate to manage risk in respect of cybersecurity and cyber resilience for itself and across its AR network.

6 RI Advice must, within 5 months of the date of these Orders, provide the plaintiff with a written report of a suitably qualified independent expert (**Expert**) confirming RI's compliance with paragraph 5 above.

7 The identity of the Expert and the terms of his or her retainer are to be agreed between the plaintiff and RI Advice, or failing agreement are to be determined by the Court.

8 The Expert is to commence their work by no later than 3 months from the date of these Orders.

9 The costs of the Expert are to be paid by RI Advice.

Other orders

10 RI Advice pay the plaintiff's costs.

11 Such further or other orders as the Court thinks fit.

Date: 21 October 2021

Signed by Andrew John Christopher

Lawyer for the plaintiff

This pleading was prepared by Fleur Shand of counsel and settled by Peter Collinson QC, Stephen Parmenter QC and Paul Liondas of counsel.

Certificate of lawyer

I Andrew John Christopher certify to the Court that, in relation to the statement of claim 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 October 2021

Signed by Andrew John Christopher

Lawyer for the plaintiff