FEDERAL COURT OF AUSTRALIA

Australian Securities and Investments Commission v FIIG Securities Limited [2026] FCA 92

File number:	QUD 144 of 2025
Judgment of:	**DERRINGTON J**
Date of judgment:	13 February 2026
Catchwords:	**CORPORATIONS** – Financial services licence – ASIC sought declaration under s 1317E(1) of the *Corporations Act 2001* (Cth) (*Corporations Act*) in respect of admitted contraventions of s 912A of the *Corporations Act* – ASIC sought orders imposing a pecuniary penalty in an agreed sum – where defendant was subject to a cyber attack as a result of it failing to establish and maintain adequate cybersecurity measures – whether defendant failed to do all things necessary to provide financial services efficiently, honestly and fairly – whether defendant failed to have available adequate financial, technological and human resources to provide financial services – whether defendant failed to have adequate risk management systems – whether appropriate to grant penalty jointly sought – orders made
Legislation:	*Corporations Act 2001* (Cth) *Crimes Act 1914* (Cth *Evidence Act 1995* (Cth) *Privacy Act 1988* (Cth) *Taxation Administration Act 1953* (Cth) *Privacy (Tax File Number) Rule 2015* (Cth)
Cases cited:	*Australian Securities and Investments Commission v Lanterne Fund Services Pty Ltd* [2024] FCA 353 *Australian Building and Construction Commissioner v Construction, Forestry, Mining and Energy Union* (2018) 262 CLR 157 *Australian Building and Construction Commissioner v Pattinson* (2022) 274 CLR 450 *Australian Competition and Consumer Authority v Reckitt Benckiser (Australia) Pty Ltd* (2016) 340 ALR 25 *Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) (No 3)* (2020) 275 FCR 57 *Australian Securities and Investments Commission v*

AustralianSuper Pty Ltd (2025) 172 ACSR 615

Australian Securities and Investments Commission v Camelot Derivatives Pty Limited (in liq) (2012) 88 ACSR 206

Australian Securities and Investments Commission v Commonwealth Bank of Australia [2022] FCA 1422

Australian Securities and Investments Commission v RI Advice Group Pty Ltd (2022) 160 ACSR 204

Australian Securities and Investments Commission v Westpac (No 3) (2018) 131 ACSR 585

Australian Securities and Investments Commission v Westpac Banking Corporation [2019] FCA 2147

Australian Securities and Investments Commission v Westpac Securities Administration Ltd (2019) 272 FCR 170

Clean Energy Regulator v E Connect Solar & Electrical Pty Ltd (2023) 171 ACSR 216

Commonwealth v Director, Fair Work Building Industry Inspectorate (2015) 258 CLR 482

Construction, Forestry, Mining and Energy Union v Cahill (2010) 194 IR 461

Markarian v The Queen (2005) 228 CLR 357

Minister for Industry, Tourism and Resources v Mobil Oil Australia Pty Ltd (2004) ATPR ¶41,993

NW Frozen Foods Pty Ltd v Australian Competition and Consumer Commission (1996) 71 FCR 285

Trade Practices Commission v CSR Ltd (1991) ATPR ¶41-076

Division:	General Division
Registry:	Queensland
National Practice Area:	Commercial and Corporations
Sub-area:	Corporations and Corporate Insolvency
Number of paragraphs:	86
Date of hearing:	9 February 2026
Counsel for the Plaintiff:	Mr S Maiden KC, with Mr A O'Brien and Ms M Y Barnes
Solicitor for the Plaintiff:	MinterEllison
Counsel for the Defendant:	Mr M Brady KC
Solicitor for the Defendant:	Colin Biggers & Paisley

ORDERS

QUD 144 of 2025

BETWEEN:	**AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION** Plaintiff
AND:	**FIIG SECURITIES LIMITED ACN 085 661 632** Defendant

ORDER MADE BY: **DERRINGTON J**

DATE OF ORDER: **9 FEBRUARY 2026**

PENAL NOTICE

TO: FIIG SECURITIES LIMITED ACN 085 661 632

IF YOU (BEING THE PERSON BOUND BY THIS ORDER):

(A) REFUSE OR NEGLECT TO DO ANY ACT WITHIN THE TIME SPECIFIED IN THIS ORDER FOR THE DOING OF THE ACT; OR

(B) DISOBEY THE ORDER BY DOING AN ACT WHICH THE ORDER REQUIRES YOU NOT TO DO;

YOU WILL BE LIABLE TO IMPRISONMENT, SEQUESTRATION OF PROPERTY OR OTHER PUNISHMENT.

ANY OTHER PERSON WHO KNOWS OF THIS ORDER AND DOES ANYTHING WHICH HELPS OR PERMITS YOU TO BREACH THE TERMS OF THIS ORDER MAY BE SIMILARLY PUNISHED.

THE COURT NOTES THAT:

In these Orders, "Business Day" means a day (other than Saturday, Sunday or public holiday) on which market participants are open for general business in Brisbane.

THE COURT DECLARES THAT:

1. Pursuant to s 1317E of the *Corporations Act 2001* (Cth) (*Corporations Act*), at all times during the period between 13 March 2019 and 8 June 2023 the defendant (FIIG) failed to:

   (a) have available the technological resources:

      (i) comprising the "Adequate Cybersecurity Measures" (as that term is defined in the Statement of Agreed Facts and Admissions dated 23 January 2026) (Adequate Cybersecurity Measures); and

      (ii) necessary to comply with its legal obligations;

   (b) have available human resources with the skills, responsibility and capacity necessary to:

      (i) put in place and maintain the Adequate Cybersecurity Measures;

      (ii) implement the controls identified and established as part of its risk management system to mitigate the cybersecurity risks it faced;

      (iii) ensure that it complied with its legal obligations;

   (c) provision sufficient financial resources to enable FIIG to:

      (i) have in place the Adequate Cybersecurity Measures;

      (ii) put in place the human resources (either within the organisation or outsourced from a third party) with the skills, responsibility and capacity necessary to:

         1. have in place the Adequate Cybersecurity Measures;

         2. implement the controls identified and established as part of its risk management system to mitigate the cybersecurity risks it faced;

         3. ensure that it complied with its legal obligations;

   and thereby failed to have available adequate resources (including financial, technological and human resources) to provide the financial services covered by its Australian Financial Services Licence (number 224659) (Licence) as required under s 912A(1)(d) of the Corporations Act, and thereby contravened s 912A(5A) of the *Corporations Act*.

2. Pursuant to s 1317E of the Corporations Act, at all times between 13 March 2019 and 8 June 2023, FIIG failed to implement the controls identified in its risk management system to mitigate the cybersecurity risks it faced, and thereby failed to have adequate risk management systems as required under s 912A(1)(h) of the *Corporations Act*, and thereby contravened s 912A(5A) of the *Corporations Act*.

3. Pursuant to s 1317E of the *Corporations Act*, at all times during the period of 13 March 2019 to 8 June 2023, by reason of FIIG's failures to:

   (a) have in place the Adequate Cybersecurity Measures;

   (b) have available adequate financial, technological and human resources to provide the services under the Licence; and

   (c) have adequate risk management systems;

   the defendant failed to do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly as required under s 912A(1)(a) of the *Corporations Act*, and thereby contravened s 912A(5A) of the *Corporations Act*.

THE COURT ORDERS THAT:

Penalty

4. Within 30 days of this order, FIIG pay to the Commonwealth a pecuniary penalty of $2.5 million in respect of FIIG's contraventions of s 912A(5A) of the *Corporations Act*.

Compliance programme

5. Pursuant to section 1101B(1) of the *Corporations Act*, FIIG is required to undertake a compliance programme (Compliance Programme) which involves the following steps:

   (a) Within 90 days of the date of these Orders or such other time as agreed in writing between the plaintiff (ASIC) and FIIG, FIIG will engage an expert as agreed between FIIG and ASIC, each party acting reasonably (Independent Expert);

   (b) If the Independent Expert cannot, for any reason, complete the engagement contemplated by these Orders, then ASIC and FIIG must agree to the appointment of another independent expert to carry out any outstanding work and that expert will be required to carry out any outstanding work in accordance with the terms of this Order;

(c) FIIG will provide a copy of these Orders to the Independent Expert and instruct the Independent Expert to prepare a written report (First Report) which identifies what, if any, further documentation, resources and controls in respect of cyber security and cyber resilience are necessary for FIIG to implement, to reasonably manage risk in respect of cyber security and cyber resilience (Remedial Actions);

(d) FIIG will instruct the Independent Expert to deliver the First Report within 45 Business Days of the engagement of the Independent Expert or such other time as agreed with ASIC and the Independent Expert in writing, and notify ASIC as soon as reasonably practicable of any anticipated delay in the delivery of the First Report;

(e) The Independent Expert will provide a copy of the First Report to ASIC within 7 business days of the First Report being delivered to FIIG by the Independent Expert;

(f) If Remedial Actions are identified in the First Report, within 15 business days of the First Report being provided to ASIC, FIIG must, in consultation with the Independent Expert and ASIC, agree a timetable for the implementation of the Remedial Actions, including an end date by which all Remedial Actions must be completed (Agreed Date). The Agreed Date must be the earliest date reasonably practicable for the implementation of all of the Remedial Actions, or such other date as agreed in writing between ASIC and FIIG;

(g) FIIG must commence implementing the Remedial Actions no later than 45 days once the Agreed Date has been determined, unless agreed to between ASIC and FIIG in writing, and complete the implementation of the Remedial Actions by the Agreed Date;

(h) If the implementation of the Remedial Actions is likely to be delayed, FIIG must notify ASIC as soon as practicable and obtain its written confirmation to amend the Agreed Date, which must not be unreasonably withheld and/or delayed;

(i) Within 90 to 180 days after the Agreed Date, or such other later time as agreed by ASIC in writing, the Independent Expert must deliver a further written report to FIIG which reports on the outcome of the implementation of the Remedial Actions, including whether, and to what extent, the Remedial Actions have been fully and appropriately implemented (Final Report); and

(j) FIIG will provide to ASIC, within 10 days of the Final Report or such other date as agreed by ASIC in writing, an attestation from the Chief Executive Officer of FIIG, stating that they have read and understood the First and Final Reports and having made reasonable enquiries, believes the Remedial Actions have been implemented and is satisfied with how the Remedial Actions have been implemented.

6. The engagement of the Independent Expert referred to in paragraph 5(a) will require:

(a) the costs for the Independent Expert including any fees and disbursements and the implementation of any Remedial Actions to be paid by FIIG;

(b) FIIG to provide all reasonable assistance to the Independent Expert to enable the Independent Expert to conduct the work required for the purposes of the Compliance Programme, including the provision of any documents or information reasonably requested by the Independent Expert, access to relevant subject matter experts, systems and premises; and

(c) FIIG to provide a copy of any written correspondence between FIIG and the Independent Expert, as requested by ASIC from time to time other than any documents or information subject to a claim of legal professional privilege.

7. The engagement terms must include:

(a) approval from ASIC on the appointment of the selected Independent Expert and the engagement terms, which must not be unreasonably withheld and/or delayed;

(b) terms which make provision for circumstances where an actual or potential conflict of interest arises in relation to the Independent Expert;

(c) an acknowledgement that ASIC may request a copy of any written correspondence between FIIG and the Independent Expert, from time to time other than any documents or information subject to a claim of legal professional privilege;

(d) an acknowledgement that ASIC may from time to time publicly report on the progress of the Compliance Programme (for the avoidance of doubt, ASIC will not publish the First or Final Reports, or any other information where public disclosure may unduly pose a risk or threat to FIIG from a cyber security perspective); and

(e) that the terms of engagement may only be varied with the agreement of ASIC.

Costs

8. Within 30 days of this order, FIIG pay ASIC $500,000 towards ASIC's costs of and incidental to the proceeding.

Note: Entry of orders is dealt with in Rule 39.32 of the *Federal Court Rules 2011*.

REASONS FOR JUDGMENT

DERRINGTON J:

Introduction

1 This application was brought by the Australian Securities and Investments Commission (ASIC) against the defendant, FIIG Securities Limited (FIIG), for certain orders relating to alleged contraventions of obligations arising under the *Corporations Act 2001* (Cth) (the Act). The parties presented a joint Statement of Agreed Facts and Admissions to the Court as well as joint submissions addressing the issues of contravention and relief. The orders agreed upon by the parties were acceptable to the Court, and were made on 9 February 2026 at the hearing of the application. These are the reasons for the making of those orders.

2 The catalyst for ASIC's action was that from 19 May 2023, FIIG's information technology systems were subject to a cyberattack, a consequence of which was that approximately 385GB of data, which included personal information of FIIG's clients, was downloaded from its servers. Subsequently, screenshots of two documents containing some of that client information were published on the dark web. This incident was referred to by the parties in their submissions as the "Cyber Attack", and that nomenclature will be used herein. Following the occurrence of the Cyber Attack, ASIC conducted investigations, and its general allegations are that between 13 March 2019 and 8 June 2023 (the Relevant Period), FIIG failed to take adequate steps to protect itself and its clients against cybersecurity risks, such that it thereby exposed itself and them to those risks to an unreasonable extent.

3 FIIG has acknowledged that its conduct contravened subparagraphs 912A(1)(a), (d) and (h) and s 912A(5A) of the Act.

4 It might be observed, at this point, that the mere fact of a successful cyberattack on an entity's information technology systems does not necessarily indicate that the entity had failed to meet the statutory obligations imposed upon it concerning the protection of its information. It is notorious that certain countries hostile to Australia support the conduct of cyber attacks upon Australian companies and, necessarily, fund those malefactors to a large degree. It would be all but impossible to prevent every cyber attack. However, ASIC's very legitimate concern does not seek to impose an unattainable standard of information protection. Rather, ASIC is concerned that entities which are subject to obligations under the Act have adequate cyber protection systems in place.

5 As mentioned, the parties have reached consensus upon a Statement of Agreed Facts and Admissions pursuant to s 191 of the *Evidence Act 1995* (Cth) for the purposes of these proceedings. To that extent, FIIG admits the facts set out in that statement and makes admissions as to the contraventions during the Relevant Period.

Background

6 FIIG is the holder of an Australian Financial Services Licence (AFSL), which authorises it to engage in dealing with fixed income financial products and services. During the Relevant Period, it was entitled to provide financial product advice, deal in financial products, make a market for certain financial products, and provide custodial or depository services.

7 In the course of its business, it collected and maintained personal information about its clients including their names, addresses, dates of birth, phone numbers, email addresses, details of driver's licences, passports and Medicare cards, Tax File Numbers, Australian Business Numbers and bank account details. In the proceedings this information is referred to as the "Personal Client Information".

8 In addition, FIIG maintained electronic records of its clients' individual fixed income investments and stored that data on its internal servers. It also managed outward-facing electronic platforms through which (a) clients could access information about their investments, and (b) investments could be bought and sold.

9 Over the Relevant Period:

(a) the value of assets under FIIG's control for its clients ranged between approximately $2.99 billion and $3.7 billion; and

(b) the value of funds under advice ranged between $4.7 billion and $7.6 billion.

10 As part of its relations with clients, FIIG warranted in its "Client Custody Agreement Terms and Conditions" that it had the capacity to perform the core administrative activities in relation to the custodial services it offered, which included having "computer systems which are secure". It also agreed with its clients to take reasonable steps to keep secure all confidential information in its possession.

11 The parties have agreed that given the nature and extent of FIIG's business, including the value of the assets under its control, there was a real risk that:

(a) FIIG could be the subject of a cyber attack;

(b) such a cyber attack could lead to adverse consequences for FIIG and its clients, including:

(i) an unauthorised party accessing Personal Client Information;

(ii) the unauthorised download, publication, modification or deletion of data stored by FIIG;

(iii) FIIG's network or computer system being disabled;

(iv) FIIG losing the ability to view or meaningfully deal with information or data which it stored;

(v) loss of FIIG's ability to provide financial services covered by its licence;

(vi) an unauthorised party being enabled to impersonate FIIG's clients or employees in dealing with FIIG or third parties; and

(vii) financial loss; and

(c) a cyber attack on FIIG could result in one or more of the following additional adverse consequences:

(i) an unauthorised party viewing FIIG's confidential information and trade secrets;

(ii) FIIG becoming subject to proceedings for breaches of the obligations that FIIG owed to its clients; and

(iii) significant reputational damage.

The above were referred to by the parties as the "Cybersecurity Risks" and that term will be used in these reasons.

12 At all times through the Relevant Period, FIIG was aware of the existence of the Cybersecurity Risks. Had they materialised, it was at risk of claims being made against it pursuant to a number of pieces of legislation, including the *Privacy Act 1988* (Cth), the *Privacy (Tax File Number) Rule 2015* (Cth) and the *Taxation Administration Act 1953* (Cth).

13 The impact of the materialisation of the Cybersecurity Risks was capable of being reduced by FIIG adopting appropriate measures to improve its cybersecurity and cyber resilience.

FIIG's obligations under the Act

14 As an AFSL holder, during the Relevant Period, FIIG was subject to obligations under subparagraphs 912A(1)(a), (d) and (h) of the Act. A person who contravenes those will also contravene s 912A(5A), which is a civil penalty provision: see s 1317E of the Act.

15 The obligations referred to above have been the subject of judicial consideration over an extended period of time, and their nature and scope are fairly clearly delineated. Such matters were carefully and accurately canvassed by the parties in their joint submissions, the substance of which is as follows:

(1) Subparagraph 912A(1)(a) requires the doing of "all things necessary to ensure" that financial services are provided "efficiently, honestly and fairly", which:

(a) does not impose a standard of perfection, but is a forward-looking standard, directed to the taking of steps to achieve compliance with the statutory norm: *Australian Securities and Investments Commission v AustralianSuper Pty Ltd* (2025) 172 ACSR 615, 640 [143]; *Australian Securities and Investments Commission v Commonwealth Bank of Australia* [2022] FCA 1422 [146], [151] – [152];

(b) has been described as "compendious", requiring that licensees "go about their duties efficiently having regard to the dictates of honesty and fairness, honestly having regard to the dictates of efficiency and fairness, and fairly having regard to the dictates of efficiency and honesty": *Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) (No 3)* (2020) 275 FCR 57, 148 [506] (*ASIC v AGM Markets*); cf *Australian Securities and Investments Commission v Westpac Securities Administration Ltd* (2019) 272 FCR 170, 266 – 267 [422] – [426] (*ASIC v Westpac Securities Administration*); and

(c) connotes (among other things) a requirement of competence in providing advice and in complying with relevant statutory obligations: *ASIC v AGM Markets* 148 [507].

(2) Under subparagraph 912A(1)(a):

(a) *efficiency* requires the licensee to be (among other things) "capable, competent and adequate", and will be absent when "performance of a licensee's functions falls short of the reasonable standard of performance … that the public is entitled to expect": *ASIC v AGM Markets* 148 – 149 [508]; *Australian*

Securities and Investments Commission v Camelot Derivatives Pty Limited (in liq) (2012) 88 ACSR 206, 225 [69(c)]; *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* (2022) 160 ACSR 204, 212 [30(f)], 214 – 215 [41] – [49] (*RI Advice*); and

(b) *fairness* contemplates conduct free from bias, dishonesty or injustice; legitimately sought or done; and proper under the rules: *ASIC v Westpac Securities Administration* 210 [174].

(3) Failing to ensure that adequate cybersecurity measures are in place can result in a failure to do all things necessary to provide financial services efficiently and fairly: *RI Advice* 217 [65].

(4) Subparagraphs 912A(1)(d) and (h) each impose a standard of *adequacy*, which is a notion that imports a normative standard of conduct against which the licensee's provision of resources and risk management systems can be judged: *RI Advice* 216 [55]; *Australian Securities and Investments Commission v Lanterne Fund Services Pty Ltd* [2024] FCA 353 [80] (*Lanterne*). For example, the assessment of "adequate risk management systems", in the context of cybersecurity, requires consideration of the risks faced by a licensee, and whether the business had "adequate" systems to manage those risks: *RI Advice* 215 – 216 [54] – [55].

Subparagraph 912A(1)(a): failure to ensure that financial services were provided efficiently, honestly and fairly

16 In the context of the foregoing discussion, ASIC has alleged, and it was admitted, that in order to do all things necessary to ensure that FIIG provided the financial services covered by its AFSL efficiently, honestly and fairly, it was required to have adequate measures in place to protect its clients from the Cybersecurity Risks.

17 The parties agreed, and it can be accepted, that the standard of competence in respect of cybersecurity, or the reasonable standard of performance that the public is entitled to expect, should be informed by:

(a) the nature of FIIG's business (including its size and resources);

(b) the Personal Client Information it held;

(c) the value of the funds under advice and the assets held by it on behalf of clients;

(d) the magnitude and potential consequences of the Cybersecurity Risks; and

(e) FIIG's contractual obligations to its clients.

18 Taking into account those matters, FIIG ought to have had in place a regime of cybersecurity measures which was appropriate to its circumstances. In the Statement of Agreed Facts and Admissions, the parties identified a number of areas in which FIIG's arrangement fell short of what might be said to be adequate cybersecurity measures. Though FIIG did have in place a regime of measures, they were insufficient to provide adequate protection given the level of Cybersecurity Risks.

Inadequacy of FIIG's Cybersecurity Measures

19 The parties agree that FIIG's cybersecurity measures were inadequate in a number of respects. Those inadequacies were articulated by the parties in the Statement of Agreed Facts and Admissions as follows.

20 In the period from 13 March 2019 to around January 2023, FIIG did not have in place a cyber incident response plan which:

(a) identified the action to be taken by FIIG to:

(i) detect and confirm the occurrence of a cybersecurity incident;

(ii) contain the incident;

(iii) identify the cause of the incident and take steps to eliminate the cause or prevent its repetition; and

(iv) return the system to normal operations (whilst ensuring the integrity and confidentiality of information);

(b) identified the FIIG personnel to be contacted in the event of a cyber incident; and

(c) was tested by FIIG at least annually.

21 Between 13 March 2019 and at least 13 February 2023, particular FIIG user accounts that were used for privileged access and tasks:

(a) were also used for non-privileged access and tasks;

(b) were not required to be a minimum of 14 characters; and

(c) were protected by passwords which were recorded in files on FIIG's network, and therefore not stored using secure methods.

22 Throughout the Relevant Period, FIIG did not review access rights to ensure that they were appropriate on a quarterly basis.

23 FIIG did not, at any time during the Relevant Period:

(a) have a network-based scanning tool which was capable of identifying security vulnerabilities in FIIG's network;

(b) have software on all endpoints capable of identifying security vulnerabilities on those endpoints;

(c) run vulnerability scans over its network and endpoints; or

(d) review the results of any vulnerability scans and take action to address any vulnerabilities identified.

24 Throughout the Relevant Period, FIIG only conducted:

(a) external penetration testing of its perimeter, network and some of its applications in and about February 2023; and

(b) vulnerability testing related to its website in or about 2021.

25 Throughout the Relevant Period, FIIG did not carry out penetration testing of:

(a) FIIG's external perimeter, internal network and at least business-critical applications at least annually; or

(b) systems and applications in FIIG's network that were:

(i) identified as having an increased risk profile; or

(ii) introduced into FIIG's network or the subject of a significant change,

at or about the time that the matter referred to in (i) or (ii) occurred.

26 At all times throughout the Relevant Period, FIIG had Palo Alto "next generation" firewalls (FIIG's Firewalls) in place.

27 At all times throughout the Relevant Period, FIIG's Firewalls were not configured to:

(a) prevent endpoints or servers from establishing direct connections to file transfer protocol servers over the internet; or

(b) restrict access to the internet from internal systems to only the extent necessary to perform those systems' respective roles within the business.

28 At all times throughout the Relevant Period, the only limit that FIIG's Firewalls imposed on the protocols which could be used by outbound traffic to connect to the internet was a restriction on email accessing Simple Mail Transfer Protocols.

29 Between 13 March 2019 and at least 13 February 2023, FIIG did not configure group policies on the Active Directory to disable insecure New Technology LAN (local area network) Manager version 1 (NTLMv1) hash authentication on all endpoints and servers.

30 From in or about July 2019, FIIG had installed EDR software "Carbon Black" on some, but not all, of its endpoints and servers.

31 At all times throughout the Relevant Period, FIIG:

(a) had Carbon Black Agents which were more than two versions behind the current version of the software, in circumstances where there were no known defects in subsequent versions of the software; and

(b) did not update threat signatures at least daily.

32 FIIG did not, at any time during the Relevant Period:

(a) monitor the alerts produced by Carbon Black on a daily basis; or

(b) monitor or arrange for monitoring of the Carbon Black alerts on a daily basis by a person with sufficient skills, training and experience to identify and respond to any unusual network activity.

33 FIIG did not, at any time during the Relevant Period, tune Carbon Black to suppress alerts generated by activities which were known to be nonthreatening.

34 Throughout the Relevant Period, or alternatively between 13 March 2019 and at least 13 February 2023, FIIG did not:

(a) have a patching plan across its systems and applications to identify available patches and software updates;

(b) apply patches to all applications, operating systems and firmware capable of being patched by no later than:

(i) 30 days after release of the patch or update for critical or high importance patches;

(ii) 90 days after release of the patch or update for medium importance patches; or

(iii) 12 months for all other patches; or

(c) update all operating systems to at least a version currently supported by the vendor; or

(d) apply additional compensating controls in respect of operating systems and applications which could not be updated, to control the increased risk of compromise.

35 Between 13 March 2019 and at least 13 February 2023, FIIG did not apply a security patch to correct the security vulnerability known as "EternalBlue".

36 Between 14 May 2019 and at least 29 May 2023, FIIG did not apply a security patch to correct the security vulnerability known as "Blue Keep".

37 FIIG did not have multi-factor authentication for its remote access users from late 2022.

38 FIIG did not at any time during the Relevant Period, have a practice of monitoring threat alerts by IT personnel with the knowledge, skills and experience to identify and respond to any unusual or suspicious activity.

39 Throughout the Relevant Period, the only cybersecurity awareness training FIIG provided to its employees was:

(a) informing staff, during induction training, of the existence of FIIG's policies, including its IT Information Security Policy and Cyber and Information Security Policy; and

(b) two emails sent from FIIG's Chief Operating Officer to all FIIG employees in 2022 concerning phishing or "spam" emails.

40 FIIG did not at any time during the Relevant Period:

(a) provide mandatory security awareness training to employees addressing the organisation's key cybersecurity risks and the behaviour expected of employees in respect of those risks; or

(b) have processes in place to ensure that training of the type described in subparagraph (a) above occurred on an annual basis.

41 FIIG did not at any time during the Relevant Period have a process or processes to review and evaluate:

(a) the effectiveness of existing technical cybersecurity controls on at least:

(i) a quarterly basis for EDR configuration and rules; and

(ii) an annual basis for all other controls; or

(b) FIIG's cyber resilience across the organisation on at least an annual basis.

42 As can be seen, in the context of the circumstances of this case, agreement has been reached that the cybersecurity measures which were in place fell short of the standard required. That appropriate level of cybersecurity inferentially appears from the matters articulated above.

43 The conclusion that, during the Relevant Period, FIIG did not have adequate cybersecurity measures in place means that it thereby contravened subparagraph 912A(1)(a) and, in turn, s 912A(5A) of the Act.

Subparagraph 912A(1)(d): failure to have available adequate resources

44 Again, ASIC alleges and FIIG acknowledges that, in order for the latter to meet its obligations under subparagraph 912A(1)(d) of the Act, it was required to have available technological, human and financial resources:

(a) comprising adequate cybersecurity measures (see *supra* [20] – [42]);

(b) necessary to ensure that it had adequate cybersecurity measures in place; and

(c) necessary to comply with its legal obligations, relevantly including under subparagraphs 912A(1)(a) and (h).

45 In relation to the adequacy of its technological resources, by reason of FIIG failing to have adequate cybersecurity measures throughout the Relevant Period (see *supra* [20] – [42]), it consequentially failed to comply with its obligations under subparagraphs 912A(1)(a) (see *supra* [43]) and (h) (see *infra* [51] – [54]).

46 In relation to its obligations to have available human resources, FIIG was required to employ or outsource from third parties, people with the skills, knowledge and experience in IT security measures to ensure that it had in place:

(a) adequate cybersecurity measures; and

(b) the measures identified as controls in FIIG's risk management system.

47 In addition, FIIG needed to ensure that sufficient staff or contractors were given a sufficient level of responsibility for carrying out those tasks and with sufficient time to properly discharge them. The parties agreed that FIIG met neither of those requirements.

48 Throughout the Relevant Period, FIIG delegated operational responsibility for its IT security to its Chief Operating Officer, and also employed some IT staff. Though it employed between 9 and 14 IT staff during the relevant period, those individuals were not possessed of sufficient skills, knowledge or experience in IT security, and nor did they have sufficient time – having regard to their other responsibilities within the organisation – to ensure that FIIG had the necessary measures in place.

49 In relation to the adequacy of financial resources, it is readily concluded, and FIIG has acknowledged, that it did not provision sufficient financial resources to enable it to have adequate cybersecurity measures in place, or to employ or outsource the human resources which are referred to above.

50 As a result of the foregoing, it failed to meet its obligations under subparagraph 912A(1)(d) of the Act, thereby contravening s 912A(5A).

Subparagraph 912A(1)(h): failure to have adequate risk management systems

51 In relation to the obligations imposed by subparagraph 912A(1)(h) of the Act, in order for FIIG to have "adequate risk management systems" to protect itself and its clients from the Cybersecurity Risks, it was required to:

(a) identify and evaluate those risks;

(b) identify, establish, fully implement and maintain controls adequate to manage or mitigate those risks; and

(c) monitor those controls to ensure that they were effective.

52 Relevantly, the parties agreed that FIIG failed to meet its obligations in two respects. The first was that it failed to sufficiently put in place adequate cybersecurity measures to manage or mitigate the Cybersecurity Risks. That said, they agreed that the declarations in relation to subparagraph 912A(1)(h) ought not include any declaration in this respect.

53 However, the second manner in which FIIG failed to meet its obligations under subparagraph 912A(1)(h) was that it failed to fully implement, maintain, and monitor those controls which it had adopted under its risk management system. In particular, the parties agreed that FIIG failed to fully implement some of the procedures and controls set out in its IT Information Security Policy, its Cyber and Information Security Policy, and its annual audits of custodial services, each of which formed part of its risk management system.

54 FIIG admits that by reason of these identified failings, it failed to have adequate risk management systems in place and thus contravened subparagraph 912A(1)(h) and, in turn, s 912A(5A) of the Act.

Legal principles on relief sought by agreement

55 The parties seek, by agreement, both declarations and orders imposing pecuniary penalties in respect of FIIG's various contraventions of the Act. It is now well accepted that courts should not be reluctant to act upon agreements reached by regulators and those whom they regulate, as to the occasion of a relevant statutory contravention and the quantum of any penalty that should be imposed: *Commonwealth v Director, Fair Work Building Industry Inspectorate* (2015) 258 CLR 482, 503 – 508 [46] – [61] (*Commonwealth v Director, Fair Work Building Industry Inspectorate*); see also *NW Frozen Foods Pty Ltd v Australian Competition and Consumer Commission* (1996) 71 FCR 285, 291; *Minister for Industry, Tourism and Resources v Mobil Oil Australia Pty Ltd* (2004) ATPR ¶41,993, 48,626 [51]; *Clean Energy Regulator v E Connect Solar & Electrical Pty Ltd* (2023) 171 ACSR 216, 234 – 237 [33] – [40].

56 In *Commonwealth v Director, Fair Work Building Industry Inspectorate* at 503 – 504 [46], the joint judgment of French CJ, Kiefel, Bell, Nettle and Gordon JJ emphasised that there is:

> … an important public policy involved in promoting predictability of outcome in civil penalty proceedings … which … assists in avoiding lengthy and complex litigation and thus tends to free the courts to deal with other matters and to free investigating officers to turn to other areas of investigation that await their attention.

57 Subsequently, their Honours went on to observe, at 507 [58]:

> Subject to the court being sufficiently persuaded of the accuracy of the parties' agreement as to facts and consequences, and that the penalty which the parties propose is *an* appropriate remedy in the circumstances thus revealed, it is consistent with principle and … highly desirable in practice for the court to accept the parties' proposal and therefore impose the proposed penalty.
>
> (Emphasis in original).

58 This principle is not confined to submissions on penalties, but applies equally to all forms of relief: *Lanterne* [102] – [103]. It should thus be followed in the present case when evaluating the agreed position between ASIC and FIIG.

Declarations

59 In this case, FIIG has acknowledged that it failed to comply with its obligations under subparagraphs 912A(1)(a), (d) and (h) of the Act, and it and ASIC have jointly demonstrated

with evidence that such acknowledgements were rightly made. In those circumstances, it is appropriate to make declarations, under s 1317E(1) of the Act, that FIIG, by virtue of its non-compliance with those provisions, has contravened the civil penalty provision in s 912A(5A).

60 Those declarations appear as orders 1, 2 and 3 of the orders that were made at the hearing.

Pecuniary penalties

61 Consequent upon declaring that a civil penalty provision has been contravened, the Court is entitled to make an order imposing a pecuniary penalty on the contravener: see s 1317G(1) of the Act.

62 In this matter, the parties jointly submit that a penalty of $2.5 million is appropriate. For the reasons which follow, that amount should be adopted.

Legal principles relevant to penalty

63 The submissions advanced by the parties in their joint written submissions carefully and accurately identify the broad principles to be applied when considering the amount of an appropriate penalty. In summary, they are as follows:

(1) Deterrence is the paramount consideration. Civil penalties are imposed "primarily, if not solely, for the purpose of deterrence": *Australian Building and Construction Commissioner v Pattinson* (2022) 274 CLR 450, 459 [15] (*Pattinson*).

(2) Civil penalty provisions have a "statutory function of securing compliance": *Commonwealth v Director, Fair Work Building Industry Inspectorate* 495 [24].

(3) The object of a civil penalty is "to attempt to put a price on contravention that is sufficiently high to deter repetition by the contravener and by others who might be tempted to contravene the Act": *Trade Practices Commission v CSR Ltd* (1991) ATPR ¶41-076, 52,152 (*TPC v CSR*); *Commonwealth v Director, Fair Work Building Industry Inspectorate* 506 [55]. In this way, the "sting or burden" which the penalty imposes on the contravener secures both general and specific deterrence: *Australian Building and Construction Commissioner v Construction, Forestry, Mining and Energy Union* (2018) 262 CLR 157, 195 – 196 [116].

(4) In determining the penalty, the Court must take into account "all relevant matters", including those expressly listed in s 1317G(6) of the Act.

(5) Other relevant considerations were identified by French J in *TPC v CSR* at 52,152 – 52,153, and Beach J in *Australian Securities and Investments Commission v Westpac (No 3)* (2018) 131 ACSR 585, 594 [49]. The Court's task is to identify and balance all of the relevant factors and make a value judgment as to the appropriate penalty (*Australian Securities and Investments Commission v Westpac Banking Corporation* [2019] FCA 2147 [261]; *Pattinson* 460 – 461 [19]) – a process described as "instinctive synthesis": *Australian Competition and Consumer Authority v Reckitt Benckiser (Australia) Pty Ltd* (2016) 340 ALR 25, 37 – 38 [44].

(6) In fixing the appropriate penalty, the Court must also have regard to the maximum penalty for the contravention, which provides a "yardstick" to be balanced with all other relevant factors: *Markarian v The Queen* (2005) 228 CLR 357, 372 [31]; *Pattinson* 471 – 472 [52] – [55].

(7) Where the penalty is imposed for multiple contraventions, and there is an interrelationship between their legal and factual elements, the Court may also have regard to the "course of conduct" principle (*Pattinson* 484 [96]) which permits the penalty to be adjusted to ensure that the contravener is not punished twice for the same conduct: *Construction, Forestry, Mining and Energy Union v Cahill* (2010) 194 IR 461, 473 – 474 [39] – [42].

(8) Ultimately, the objective of the Court in the imposition of a penalty is to ensure, as a matter of totality, that the overall penalty is "just and appropriate": *Pattinson* 483 [94].

Application in the present case

64 The parties agreed that the maximum penalty for each contravention in this case by a body corporate is that prescribed in s 1317G(4) of the Act. They agreed that the maximum penalty is calculated under s 1317G(4)(a), being 50,000 penalty units.

65 Further, they provided the following table as indicating the value of one penalty unit under s 4AA of the *Crimes Act 1914* (Cth) as it varied over the Relevant Period:

Date of conduct	Value of one PU	50,000 PUs	2½ million PUs
13 March 2019 to 30 June 2020	$210	$10,500,000	$525 million
1 July 2020 to 31 December 2022	$222	$11,100,000	$555 million
1 January 2023 to 8 June 2023	$275	$13,750,000	$687.5 million

66 As the parties agreed, FIIG committed three contraventions of s 912A(5A) – being one for each contravention of subparagraphs 912A(1)(a), (d) and (h) – which results in the maximum penalty being $41,250,000.

67 Despite that, there is a close interrelationship between each of the contraventions, being that each arises (partly or wholly) from FIIG's failure to have in place adequate cybersecurity measures, and each forms part of a single "course of conduct". That said, a factually distinct form of conduct arises from FIIG's failure to fully implement and monitor the measures identified in its risk management system.

68 Whilst the available maximum penalty is an important metric, the course of conduct principle indicates that a penalty at or near the maximum is not appropriate in this case.

Nature and extent of the contraventions

69 The parties accept that the contraventions occurred continuously over a period of approximately 4 years and 3 months, and arose as a result of FIIG's failure over the Relevant Period to adequately invest in its cybersecurity and cyber resilience, despite its awareness of the Cybersecurity Risks and the importance of the Personal Client Information which it held. That is a not insignificant consideration, though, on the other hand, it is not suggested in any way that the contraventions occurred as a result of any deliberate misconduct by FIIG.

70 It is also relevant that, despite the continuance of the contraventions over an extended period, they were not productive of loss for all that time. That is not to diminish the importance of maintaining adequate cybersecurity and cyber resilience, but merely to note that the duration of the contraventions is not the most significant element.

Nature and extent of any loss or damage suffered consequent upon the contraventions

71 Very properly, the parties have agreed upon an adequate analysis of the causal connection between FIIG's contraventions and the events as they occurred. It is agreed that if, as at 19 May 2023 (being the day of the first Cyber Attack), FIIG had had in place (a) adequate cybersecurity measures, and (b) the risk management procedures described in its risk management system, there was an increased chance that it could have detected the Cyber Attack, implemented its cyber incident response plan sooner, and prevented some or all of the Personal Client Information from being downloaded from FIIG's servers.

72 The known financial loss flowing from the Cyber Attack is largely limited to FIIG's own remediation costs which total around approximately $1,500,000.

73 Further, some of its customers suffered a compromise of their confidential Personal Client Information and, whilst it is not possible to quantify the consequence of those losses, there is potential for them to be significant. Further, the clients are placed in a difficult position knowing that their information might be used by nefarious actors.

74 The fact that the known losses consequent upon the breaches have been sustained by FIIG itself rather than others, mitigates the need for a higher penalty which might have been more appropriate if the identifiable losses were sustained by third parties. The consequences of the contraventions have been directly visited upon FIIG, which will no doubt serve to encourage it to perform its statutory obligations in the future.

Prior conduct

75 FIIG has not previously been found to have engaged in any conduct which is similar to that alleged by ASIC in this matter. Further, there is no evidence that it has previously been involved in any prior contravention of any provision of the Act.

76 The absence of any evidence of any prior similar conduct, removes any thought that FIIG will not be responsive to the imposition of a penalty, even if it is of a more modest size.

Cooperation

77 It is significant that, in this matter, FIIG has been fully cooperative with ASIC by engaging from any early stage in good faith discussions to resolve the proceedings, making admissions, assisting in the preparation of the Statement of Agreed Facts and Admissions, and agreeing on the making of joint submissions. That conduct has avoided the need for a contested trial which would, no doubt, have been substantive and expensive. That has the corollary that the resources of ASIC and the Court are freed up and that promotes an important public policy objective.

78 In this case, the parties have agreed that a substantial discount for cooperation is appropriate and that should be wholly endorsed.

Specific deterrence

79 The quantum of the pecuniary penalty at $2,500,000 can be compared to the financial position of FIIG as a relevant indicative factor. It represents some 20% of FIIG's net assets as at 30 June 2025, and around 8% of its turnover for the 2025 financial year. That has the consequence

that the quantum of the penalty imposed provides an appropriate "sting" for FIIG and renders the penalty far more than merely being a cost of doing business.

General deterrence

80 It is well accepted that the penalties imposed by the Courts should be sufficiently substantive to ensure that the contravention is not seen as being less costly than the AFSL holder complying with its obligations under s 912A(1) in respect of cybersecurity. Here, the cost of compliance over the Relevant Period would have been approximately $1.2 million and, therefore, the imposition of a penalty of $2,500,000 will validate the behaviour and efforts of compliant businesses, and will send a warning to businesses with inappropriate underinvestment in cybersecurity.

Remedial, disciplinary and compliance steps

81 Also relevant to the intuitive analysis in the quantification of the penalty is the consideration of the remedial, disciplinary and compliance steps taken. In this case, since the occurrence of the Cyber Attack, FIIG has adopted a number of steps to improve its cybersecurity and cyber resilience. In addition, the proposed orders sought by ASIC, and agreed to by FIIG, impose a compliance program which would require FIIG to engage an appropriately qualified independent expert to report on its cybersecurity posture and identify any further necessary remedial action, and to ensure that FIIG implements those remedial actions within a relatively short period of time following the report. All of this is to occur at FIIG's expense.

Conclusion as to penalty

82 For the reasons given in the course of addressing the above considerations, the penalty agreed to between the parties is appropriate.

Other orders

83 As mentioned, the parties have agreed upon further orders requiring FIIG to undertake a compliance program. Such orders fall within the Court's broad discretion under s 1101B(1) of the Act. In exercising that power, the Court is to consider:

(a) whether such an order is necessary in light of the specific circumstances of the contravention, other relief proposed to be granted, and the steps taken since the contravention;

(b) whether the compliance program has a connection with the contravening conduct; and

(c) whether it strikes the appropriate balance between prescription, so as to avoid uncertainty, and over-particularity, so as to avoid unworkability.

84 In the circumstances before the Court, the compliance program has self-evident worth and merit. It is necessary to ensure that FIIG now has the cybersecurity documentation and controls necessary to reasonably manage those risks which it faces. The program is tailored to the conduct which gave rise to the contraventions – being the failure to have in place adequate measures – and is framed at an appropriate level of detail. It also allows the specific recommendations to be developed by an independent expert and for them to be implemented on a timetable agreed between ASIC and FIIG.

85 In those circumstances, it is appropriate to make the orders referred to above requiring FIIG to undertake the compliance program, the terms of which appear in orders 5, 6 and 7.

Costs

86 The parties also jointly agree upon an order requiring FIIG to pay a contribution towards ASIC's costs of these proceedings in an amount of $500,000. In circumstances where the parties are represented by knowledgeable and experienced legal advisors, it is appropriate to accept the quantification involved in that costs order and it ought to be made.

I certify that the preceding eighty-six (86) numbered paragraphs are a true copy of the Reasons for Judgment of the Honourable Justice Derrington.

Associate: 

Dated: 13 February 2026