NOTICE OF FILING

Details of Filing

Document Lodged:	Concise Statement
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	12/03/2025 3:57:50 PM AEST
Date Accepted for Filing:	12/03/2025 4:03:00 PM AEST
File Number:	QUD144/2025
File Title:	AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION v FIIG SECURITIES LIMITED ACN 085 661 632
Registry:	QUEENSLAND REGISTRY - FEDERAL COURT OF AUSTRALIA

Registrar

Important Information

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 of the filing of the document is determined pursuant to the Court's Rules.

Form NCF1

Concise Statement

No. 2025

Federal Court of Australia

District Registry: Queensland

Division: Commercial and Corporations

IN THE MATTER OF FIIG SECURITIES LIMITED ACN 085 661 632

Australian Securities and Investments Commission

Plaintiff

FIIG Securities Limited ACN 085 661 632

Defendant

A. IMPORTANT FACTS GIVING RISE TO THE CLAIM

Introduction

1. The plaintiff (**ASIC**) alleges that between 13 March 2019 and 8 June 2023 (the **Relevant Period**), the defendant (**FIIG**) failed to take adequate steps to protect itself and its clients against cybersecurity risks, thereby exposing itself and them to those risks to a heightened and unreasonable extent. FIIG's conduct culminated in a cyber intrusion beginning on 19 May 2023, in which approximately 385GB of data, including personal information of FIIG's clients, was downloaded from FIIG's servers, some of which was published on the dark web. ASIC alleges that FIIG's conduct contravened ss 912A(1)(a), (d) and (h) and 912A(5A) of the *Corporations Act 2001* (Cth) (the **Act**).

FIIG's business and exposure to cyber risk

2. FIIG is an Australian Financial Services Licensee specialising in fixed income financial products and services. At all material times its Australian Financial Services Licence (**AFSL**) has authorised it to (in summary) provide financial product advice; deal in financial products; make a market for certain financial products; and provide custodial or depository services.

3. In the course of providing those services, FIIG has collected and maintained personal information about its clients, including all or some of their names, addresses and dates of birth; their phone numbers and email addresses; copies of driver's licenses, passports and

Filed on behalf of (name & role of party) Australian Securities and Investments Commission , Applicant
Prepared by (name of person/lawyer) Melinda Smith
Law firm (if applicable) MinterEllison
Tel 07 3119 6000 Fax 07 2807 7880
Email melinda.smith@minterellison.com
Address for service (include state and postcode) One Eagle - Waterfront Brisbane, 1 Eagle Street, BRISBANE QLD 4000
Our reference: 1502698

Medicare cards or details of those; Tax File Numbers; Australian Business Numbers; and bank account details (**Personal Client Information**).

4. During the Relevant Period, a core part of FIIG's business was the provision of custodial services. FIIG held fixed income investments on behalf of its clients. The assets that FIIG held were held by FIIG's sub-custodial service provider, JP Morgan, on an aggregated basis. However, FIIG maintained electronic records of the clients' individual fixed income investments, stored that data on its servers and managed an electronic platform through which the investments could be bought and sold. Over the Relevant Period, the value of the assets that JP Morgan held on behalf of FIIG and its clients ranged between approximately $2.89 billion to $3.7 billion. FIIG also held or controlled money on behalf of its clients – such as money paid by clients to FIIG to fund trades and coupon payments payable to those clients.

5. Given the nature of FIIG's business, the nature and extent of the information that it held, and the significant value of assets under its control, there was a real risk that: (a) FIIG would be the subject of an attempted or actual cyber intrusion; and (b) such a cyber intrusion could lead to adverse consequences for FIIG and its clients, including the viewing, downloading, publication or other use of data stored by FIIG (including Personal Client Information); loss of the ability to access or meaningfully deal with FIIG's data (e.g. by reason of its deletion or encryption); loss of the ability to operate FIIG's network or computer system or parts thereof; loss of FIIG's ability to provide financial services covered by its licence; an unauthorised party being enabled to impersonate FIIG's clients or employees in dealing with FIIG or third parties; and financial loss to FIIG (including financial losses associated with the risk of being exposed to civil penalties and claims for damages) and its clients.

FIIG's obligations under the Act

6. During the Relevant Period, as the holder of an AFSL, FIIG was subject to obligations under s 912A(1) of the Act, including obligations to: (a) do all things necessary to ensure that the financial services covered by its licence were provided efficiently, honestly and fairly: s 912A(1)(a); (b) have available adequate resources (including financial, technological, and human resources) to provide the financial services covered by its licence: s 912A(1)(d); and (c) have adequate risk management systems: s 912A(1)(h).

Failure to have adequate cybersecurity measures

7. During the Relevant Period, to meet its obligations under s 912A(1)(a), FIIG was required to have in place adequate measures to protect its clients from the risks and consequences of a cyber intrusion (**Adequate Cybersecurity Measures**). The Adequate Cybersecurity Measures that FIIG ought to have had in place relevantly included:

   (a) at least each of the measures identified in **Annexure A**; or

(b) alternatively, such of those measures as would provide adequate protection from those risks and consequences,

(collectively **the Missing Cybersecurity Measures**).

8. At various times during the Relevant Period (and in some instances, throughout that entire period) FIIG did not have many or all of the Missing Cybersecurity Measures in place.

Failure to have adequate resources

9. During the Relevant Period, to meet its obligations under s 912A(1)(d), FIIG was required to have available adequate financial, technological and human resources to:

(a) ensure that it had in place Adequate Cybersecurity Measures, relevantly including the Missing Cybersecurity Measures; and

(b) comply with its legal obligations, relevantly including under s 912A(1)(a) and (h).

10. In respect of *technological resources*, that required FIIG to have at least Adequate Cybersecurity Measures, relevantly including the Missing Cybersecurity Measures.

11. In respect of *human resources*, that required FIIG to:

(a) employ or outsource from a third party people with the skills, knowledge and experience in IT security to ensure that:

(i) FIIG had in place Adequate Cybersecurity Measures, relevantly including the Missing Cybersecurity Measures; and

(ii) the cybersecurity measures purportedly adopted by FIIG as part of its risk management system (identified in **Annexure B**, and addressed further in paragraph 16 below) were implemented; and

(b) as part of this, ensure that one or more persons were given responsibility for carrying out those tasks and sufficient time to properly discharge that responsibility.

12. In respect of *financial resources*, that required FIIG to provision sufficient financial resources to enable it to:

(a) have in place Adequate Cybersecurity Measures, relevantly including the Missing Cybersecurity Measures;

(b) have the human resources described in paragraph 11 above; and

(c) implement the risk management measures identified in Annexure B.

13. During the Relevant Period, FIIG did not have available the financial, technological and human resources identified in paragraphs 9-12 above:

(a) As to *technological resources*, FIIG did not have many or all of the Missing Cybersecurity Measures.

(b) As to *human resources*, FIIG did not employ or outsource human resources to enable it to have the measures and resources pleaded in paragraph 11(a) above. FIIG substantially relied on its Chief Operating Officer and IT infrastructure team in respect of cybersecurity, but the relevant employees had a wide range of other responsibilities and were otherwise unable to ensure the adequacy of FIIG's cybersecurity measures.

(c) As to *financial resources*, FIIG did not provision sufficient financial resources to enable it have the measures and resources pleaded in paragraph 12 above.

Failure to have adequate risk management systems

14. During the Relevant Period, to meet its obligations under s 912A(1)(h), FIIG was required to have a risk management system that adequately identified and evaluated the risks faced by FIIG and its clients; adopt controls adequate to manage or mitigate those risks to a reasonable level; and implement those controls.

15. During the Relevant Period, FIIG failed to adopt controls adequate to manage or mitigate the risks to it and its clients to a reasonable level by failing to put in place and maintain the Missing Cybersecurity Measures or some of them.

16. Further or alternatively, during the Relevant Period, FIIG had a risk management system, which included an IT Information Security Policy and Cyber and Information Security Policy. However, during some or all of the Relevant Period, FIIG failed to implement measures identified in those policies, particularly the measures identified in Annexure B.

B. THE RELIEF SOUGHT FROM THE COURT

17. ASIC seeks the declaratory, pecuniary penalty and other relief set out in the accompanying originating application.

C. THE PRIMARY LEGAL GROUNDS FOR THE RELIEF SOUGHT

18. By reason of the matters described in paragraphs 9 to 13 above, during the Relevant Period, FIIG did not have available adequate resources (including financial, technological, and human resources) to provide the financial services covered by its AFSL in contravention of s 912A(1)(d) and therefore s 912A(5A) of the Act.

19. By reason of the matters described in paragraphs 14 to 16 above, during the Relevant Period, FIIG did not have adequate risk management systems, in contravention of s 912A(1)(h) and therefore s 912A(5A) of the Act.

20. By reason of the matters described in paragraphs 7 to 8 and all or some of paragraphs 9 to 16 above, during the Relevant Period, FIIG did not do all things necessary to ensure that the financial services covered by its AFSL were provided efficiently, honestly and fairly in contravention of s 912A(1)(a) and therefore s 912A(5A) of the Act.

D. HARM SUFFERED AS A RESULT OF THE CONDUCT

21. FIIG's conduct exposed FIIG and its clients to the risk of a cyber intrusion and the adverse consequences thereof to a heightened and unreasonable extent.

22. Further, on 19 May 2023, the risk of a cyber intrusion materialised. A FIIG employee inadvertently downloaded a .zip file containing malware whilst browsing the Internet. The malware allowed a threat actor to remotely access FIIG's network and perform network-based lateral movement and privilege escalation. On or about 23 May 2023, the threat actor obtained access to a privileged user account on FIIG's network and began downloading FIIG's data. Between about 23 and 30 May 2023, the threat actor downloaded approximately 385GB of data, including Personal Client Information, to an external server.

23. On 2 June 2023, the Australian Cyber Security Centre (**ACSC**) alerted FIIG that its systems may be compromised. Prior to that notification, and despite numerous firewall email alerts generated from 23 May 2023 flagging suspicious activity, FIIG had not identified or responded to the cyber intrusion. On 8 June 2023, FIIG inspected the relevant employee's laptop and (with assistance from external cybersecurity consultants) discovered that FIIG's network had been compromised and its data stolen. On 9 June 2023, FIIG took its network offline. On 10 June 2023, a threat actor published screenshots of two documents containing Personal Client Information on the dark web. FIIG was only able to restore its IT systems progressively over some months, compromising its ability to provide financial services to its clients.

24. FIIG's contraventions of one or more of ss 912A(1)(a), 912A(a)(d), 912A(1)(h) and 912A(5A) caused or contributed to severity of the incident. Had FIIG had the Missing Cybersecurity Measures in place, it would have detected suspicious activity on its network on or shortly after 19 May 2023, identified that its system had been compromised by on or about 23 May 2023, and prevented the threat actor from downloading some or all of the stolen data or, alternatively, had the opportunity to do so.

Date: 12 March 2025

This concise statement was prepared by Stewart J. Maiden KC, Angus O'Brien and Mei Barnes of Counsel.

Annexure A – Missing Cybersecurity Measures

1. A cyber incident response plan, approved by the organisation, and communicated and accessible to all employees, which:

   (a) addresses: (i) the action to be taken, key roles and responsibilities of FIIG personnel, and regulatory notification requirements, in the event of a cybersecurity event; (ii) incident detection and analysis; and (iii) incident response (containment, eradication and recovery); and

   (b) is tested by FIIG at least annually.

2. Management of privileged access to accounts on FIIG's networks, computer systems and applications to ensure that:

   (a) separate administrative accounts are used for privileged access and tasks and are not used for non-privileged activities;

   (b) those privileged accounts are subject to more complex password requirements than those for non-privileged accounts, and passwords for privileged accounts are not stored using insecure methods; and

   (c) access to systems and applications is revoked when users no longer require access.

3. Vulnerability scanning:

   (a) involving the following tool(s):

      (i) a network scanner capable of identifying security vulnerabilities in FIIG's network; and/or

      (ii) software on all endpoints capable of identifying security vulnerabilities on those endpoints; and

   (b) involving processes by which:

      (i) the tool(s) are run on an at least quarterly basis; and

      (ii) the results of the scans are reviewed and appropriate action taken to address vulnerabilities.

4. "Next-generation" firewalls configured to impose outbound traffic rules for endpoints and servers, including rules preventing:

   (a) endpoints from accessing file transfer protocol (**FTP**) services; and

   (b) internal systems from accessing the internet (except to the extent strictly necessary to perform their role within the business).

5. Configuration of group policies on the Active Directory to disable legacy and insecure authentication protocols, such as NTLMv1 hash authentication, in respect of all endpoints and servers.

6. Endpoint Detection and Response (**EDR**) software which was:

   (a) installed on all endpoints and servers in FIIG's network;

   (b) configured to automatically download and install updates to the EDR software; and

   (c) monitored on a daily basis (either directly, or through Security Incident Events Management (**SIEM**) software referred to in paragraph 9 below) by a person with sufficient skills, training and experience to identify and respond to any unusual network activity.

7. In respect of patching and software updates:

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

   (b) a practice of ensuring that patches and software updates were applied to all applications, operating systems and firmware capable of being patched by no later than:

      (i) 1 month after release of the patch or update for critical or high importance patches;

      (ii) 3 months after release of the patch or update for all other patches;

   (c) a practice of updating all operating systems to at least a version currently supported by the vendor; and

   (d) a practice of applying additional compensating controls to systems which cannot be updated or patched, to control the increased risk of compromise.

8. From in or about 2022, multi-factor authentication for all remote access users.

9. SIEM software configured to:

   (a) collect and consolidate, in real time, the security information logged across FIIG's systems, including the logs produced by the controls identified in paragraphs 4, 5 and 6 above, to a central location;

   (b) undertake analysis of those logs to identify suspicious activity; and

   (c) store the logs online for at least 90 days, and in an electronic archive for at least twelve months.

10. A practice of monitoring of the SIEM on a daily basis by IT personnel who had the knowledge, skills, experience and capacity to identify and respond to any unusual activity.

11. Mandatory security awareness training delivered to all employees upon starting, and thereafter annually, addressing the organisation's key cybersecurity risks and the employees' responsibilities.

12. A process or processes to review and evaluate the effectiveness of existing technical cybersecurity controls on an at least quarterly basis.

Annexure B – Missing risk management measures

The risk management measures identified and adopted under FIIG's IT Information Security Policy (between 13 March 2019 and 7 July 2019) and Cyber and Information Security Policy (from 5 July 2019 to the end of the Relevant Period) that were not implemented by FIIG during the Relevant Period were as follows:

1. Accounts with operating system administrative privileges must not be used for day-to-day activities such as email, internet browsing and application access.
2. Regular penetration or vulnerability tests of FIIG's perimeter must be performed from both internal and external points.
3. The most recent operating system and application security patches must be tested and installed as soon as practicable, according to a documented patch-management process.
4. Where possible, unused services, accounts and applications must be disabled.
5. The computing environment must be monitored at all times.
6. All event logs must be reviewed by a Security Administrator at least every 90 days.

Certificate of lawyer

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

Date: 12 March 2025

Signed by Melinda Smith
Solicitor for the Applicant