NOTICE OF FILING

Details of Filing

Document Lodged:	Statement of Claim - Form 17 - Rule 8.06(1)(a)
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	26/05/2025 4:27:20 PM AEST
Date Accepted for Filing:	26/05/2025 4:27:19 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 17
Rule 8.05(1)(a)

Statement of claim

No. QUD144 of 2025

Federal Court of Australia

District Registry: Queensland

Division: Commercial and Corporate

Australian Securities and Investments Commission

Plaintiff

FIIG Securities Limited ACN 085 661 632

Defendant

The parties

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

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

   (b) is entitled to sue in its corporate name pursuant to s 8(1)(d) of the ASIC Act.

2. The defendant (**FIIG**):

   (a) is a company registered under the *Corporations Act 2001* (Cth) (the **Act**), capable of being sued in its own name; and

   (b) since 13 March 2019, has been the holder of Australian Financial Services Licence (**AFSL**) number 224659 (**Licence**) and a financial services licensee (within the meaning of that term in s 9 of the Act).

FIIG's business and exposure to cyber risk

3. FIIG has been authorised under the Licence to carry on a financial services business:

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

(a) from 13 March 2019 to 3 March 2021, to:

(i) provide general financial product advice for the following classes of financial products:

(A) deposit and payment products;

(B) foreign exchange contracts;

(C) debentures, stocks or bonds issued or proposed to be issued by a government;

(D) interests in managed investment schemes, excluding investor directed portfolio services; and

(E) securities;

(ii) deal in a financial product by:

(A) issuing, applying for, acquiring, varying or disposing of financial products in the following classes:

(I) foreign exchange contracts; and

(II) interests in certain management investment schemes; and

(B) applying for, acquiring, varying or disposing of financial products in the classes listed at subparagraph (i) above on behalf of other persons; and

(iii) provide custodial or depository services by operating custodial or depository services other than investor directed portfolio services;

(b) from 4 March 2021 to 21 February 2023, to:

(i) provide general financial product advice to retail clients for the classes of financial products listed at subparagraph (a)(i) above;

(ii) provide financial product advice to wholesale clients only for the classes of financial products listed at subparagraph (a)(i) above;

(iii) deal in a financial product to retail and wholesale clients by:

(A) issuing, applying for, acquiring, varying or disposing of financial products in the following classes:

(I) foreign exchange contracts; and

(II) interests in certain management investment schemes; and

(B) applying for, acquiring, varying or disposing of financial products in the classes listed at subparagraph (a)(i) above on behalf of other persons; and

(iv) provide custodial or depository services by operating custodial or depository services other than investor directed portfolio services; and

(c) since 22 February 2023, to:

(i) do the matters pleaded in (b) above; and

(ii) make a market to retail and wholesale clients for the financial products listed in subparagraph (a)(i) above.

4. Since 13 March 2019, FIIG has carried on a financial services business that:

(a) involved performing acts that were authorised under the Licence; and

(b) included:

(i) dealing in financial products on behalf of other persons; and

(ii) providing custodial services.

5. Between 13 March 2019 and 8 June 2023 (the **Relevant Period**), in the course of carrying on its financial services business pursuant to the Licence, FIIG received and electronically stored (as data) personal and financial information of its current and former clients (**Personal Client Information**), relevantly including all or some of:

(a) their full names, addresses and dates of birth;

(b) their phone numbers and email addresses;

(c) copies of their driver's licenses and passports or details appearing on those documents;

(d) copies of their Medicare Cards or details appearing thereon;

(e) their Tax File Numbers;

(f) their Australian Business Numbers;

(g) their bank account details;

(h) the amount of their fixed income investments held by FIIG; and

(i) the amount of money held by FIIG on trust for them.

6. During the Relevant Period, in the course of providing financial services covered by its Licence, FIIG:

(a) held fixed income investments on behalf of its clients, which in turn were held by FIIG's sub-custodial service provider, JP Morgan Chase Bank, N.A. (**JP Morgan**), on an aggregated basis;

(b) facilitated the buying and selling of fixed income investments by FIIG's clients, including by using electronic systems;

(c) maintained electronic records of the fixed income investments that FIIG held on behalf of each of its clients, and stored that data on its servers;

(d) provided clients with access to information about their investments through an online portal; and

(e) held money on behalf of clients in one or more client trust accounts and one or more coupon trust accounts.

7. The approximate total value of:

(a) funds that FIIG had under advice between financial years 2019 and 2023 was between $4.9 billion and $7.6 billion; and

(b) assets that JP Morgan held on behalf of FIIG and its clients was, from time to time:

Period	**Total value ($AUD)**
1 January 2019 to 30 June 2019	$3.42 to $3.55 billion

1 July 2019 to 30 June 2020	$3.38 to $3.70 billion
1 July 2020 to 30 June 2021	$3.13 to $3.40 billion
1 July 2021 to 30 June 2022	$2.89 to $3.02 billion
1 July 2022 to 30 June 2023	$2.99 to $3.45 billion

8. During the Relevant Period:

(a) there was a real risk that FIIG may be the subject of a cyber attack;

(b) there was a real risk that a cyber attack on FIIG could result in:

(i) one or more of the following consequences for FIIG and its clients:

(A) an unauthorised party accessing Personal Client Information;

(B) the unauthorised download, publication, modification or deletion of data stored by FIIG, including FIIG's electronic records of the fixed income investments that it held on behalf of its clients;

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

(D) FIIG losing the ability to access its network or computer system;

(E) FIIG losing the ability (by means of encryption or otherwise) to view or meaningfully deal with information or data which it stored, including FIIG's electronic records of the fixed income investments that it held on behalf of its clients;

(F) FIIG losing the ability to provide financial services covered by the Licence;

(G) an unauthorised party being enabled to impersonate FIIG clients or employees in dealings with FIIG or client counterparties, or with other third parties;

(H) financial losses; and

(ii) in addition to the matters pleaded in 8(b)(i) above, one or more of the following consequences for FIIG:

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

(B) FIIG becoming subject to proceedings for breaches of legal obligations, which could result in liability to pay civil penalties, compensation or damages;

Particulars

FIIG owed the obligations pleaded in paragraphs 10 and 11.

Further, it had obligations under:

- section 15 of the *Privacy Act 1988* (Cth) (**Privacy Act**): (1) not to disclose personal information (Australian Privacy Principle (**APP**) 6.1); (2) not to disclose a government related identifier of an individual (such as a Medicare, driver's licence or passport number) unless the requirements of APP 9.2 are met (APP 9); and (3) to take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure (APP 11.1);

- sections 17 and 18 of the Privacy Act, r 10 of the *Privacy (Tax File Number) Rule 2015* (Cth) (**Tax File Rule**), and s 8WB(1)(c) of the *Taxation Administration Act 1953* (Cth) (**Tax Act**) not to disclose a person's tax file number other than for a purpose authorised by law; and

- sections 17 and 18 of the Privacy Act and r 11 of the Tax File Rule to take reasonable steps to protect tax file number information from misuse and loss, and from unauthorised access, use, modification or disclosure.

During the Relevant Period, civil penalties could be imposed for a breach of the APPs and the Tax File Rule under ss 13 and 13G of the Privacy Act, for a breach of s 912A(5A) under s 1317G of the

Act, and for a breach of s 8WB(1)(c) of the Tax Act under s 8ZF of the Tax Act.

Liability to pay damages or compensation could also arise: for breaches of civil penalty provisions in the Privacy Act, pursuant to s 80UA of the Privacy Act; for breaches of s 912A of the Act, pursuant to s 1317HA of the Act; and at common law, for breach of contract.

(C) significant reputational damage to FIIG; and

(c) the impact of the risks pleaded in subparagraphs (a) and (b) above (together, the **Cybersecurity Risks**) could be reduced by FIIG adopting measures to improve its cyber security and cyber resilience.

9. FIIG knew:

(a) during the Relevant Period, of the matters pleaded in paragraph 8 above;

Particulars

FIIG's knowledge is to be inferred from:

(a) emails exchanged between its Chief Risk Officer, Mr Brett Harper, and its Head of IT, Mr Rodney Vanelderan, on 11 and 15 August 2017 [FSL.0022.0001.0444];
(b) FIIG's Risk Registers dated January 2018 [FSL.0013.0002.0003]; March 2018 [FSL.0022.0001.0436]; 24 February 2021 [FSL.0028.0001.2235]; 17 March 2021 [FSL.0034.0002.7223]; 21 April 2021 [FSL.0034.0002.7224]; 18 May 2021 [FSL.0033.0001.3906]; 17 November 2021 [FSL.0034.0002.7225]; 1 February 2022 [FSL.0026.0001.0002]; 26 April 2022 [FSL.0034.0002.7266]; 5 July 2022 [FSL.0034.0002.7264]; 26 July 2022 [FSL.0034.0002.7234]; 29 July 2022 [FSL.0034.0002.7263]; 25 August 2022 [FSL.0034.0002.7233]; 22 November 2022 [FSL.0034.0002.7232]; and 25 January 2023 [FSL.0034.0002.7230];
(c) the Audit, Risk and Compliance Committee (ARCC) Paper dated July 2018, prepared by Mr Cameron Coleman and titled "Risk Register for priority items" [FSL.0033.0001.4204];

(d) the draft key risk schedule dated 24 September 2018 [FSL.0034.0002.6408];
(e) FIIG's IT Information Security Policies dated 23 April 2018 [FSL.0021.0002.0497]; 8 July 2019 [FSL.0014.0001.0231]; and 1 May 2022 [FSL.0021.0002.0524]; and
(f) FIIG's Cyber and Information Security Policies dated 5 July 2019 [FSL.0021.0002.0485] and 1 May 2022 [FSL.0012.0002.0289].

Further particulars may be provided following interlocutory steps.

(b) during the Relevant Period, that the risk of confidential information being obtained by hackers if controls were not in place was either high or likely to eventuate; and

Particulars

FIIG's knowledge is to be inferred from:

(a) FIIG's Risk Registers referred to in particular (b) at subparagraph (a) above;

(b) the document titled "Top 20 Risks Discussion – Meeting III" dated 24 September 2019 [FSL.0034.0002.7235]; and

(c) the Risk Management Report to the ARCC dated 3 November 2020 [FSL.0034.0002.7159].

Further particulars may be provided following interlocutory steps.

(c) in or about mid-2020, of an increase in cyber threats across the market.

Particulars

FIIG's knowledge is to be inferred from:

(a) the Risk Management Report to the ARCC dated 7 May 2020 [FSL.0033.0001.3874];

(b) the document titled "FIIG IT Deep Dive" dated July 2020 [FSL.0022.0001.0400]; and

(c) the document titled "Board Reporting – Risk Metrics ARCC" dated 22 July 2020 [FSL.0034.0002.7154].

Further particulars may be provided following interlocutory steps.

10. During the Relevant Period, FIIG provided its custodial services to clients pursuant to its "Client Custody Agreement Terms and Conditions", under which:

(a) by clause 15.2(c)(v), FIIG represented and warranted that, or to the effect that, it had the necessary capacity to perform the core administrative activities in relation to the custodial services, including "computer systems which are secure";

(b) by clause 17.1, FIIG agreed to "take reasonable steps to keep all Confidential Information secure and to hold all Confidential Information in strict confidence and not disclose, or cause or permit the disclosure of the Confidential Information", subject to certain exceptions;

(c) the term "Confidential Information" was defined to include "any information relating to the business, systems, operations, properties, assets or affairs of the Client or its related bodies corporate which is or has been disclosed by the Client (or its representatives) to the Custodian (or its representatives) or learnt or acquired by the Custodian (or its representatives) under or in connection with this Agreement", subject to certain exceptions; and

(d) by clause 3.11(b)(i), FIIG agreed to "maintain at all times proper internal control structures and compliance systems that are designed to… prevent any material and / or systemic breaches of this Agreement" by FIIG.

Particulars

The following versions of the Client Custody Agreement applied during the Relevant Period:

(a) Client Custody Agreement Terms and Conditions dated 16 May 2018;
(b) Client Custody Agreement Terms and Conditions dated 1 July 2020;
(c) Client Custody Agreement Terms and Conditions dated 11 March 2021;
(d) Client Custody Agreement Terms and Conditions dated 8 October 2021;
(e) Client Custody Agreement Terms and Conditions dated 2 May 2022; and

(f) Client Custody Agreement Terms and Conditions dated 15 March 2023.

FIIG's obligations as a licensee under the Act

11. Since 13 March 2019, as the holder of the Licence, FIIG has been 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)(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

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

FIIG's failure to have adequate cybersecurity measures

12. During the Relevant Period, in order to do all things necessary to ensure that FIIG provided the financial services covered by the Licence efficiently, honestly and fairly, FIIG was required to have adequate measures in place to protect its clients from the risks and consequences of a cyber attack pleaded in paragraphs 8(a) and 8(b)(i) above.

13. During the Relevant Period, in order for FIIG to have adequate measures in place to protect its clients from the risks and consequences of a cyber attack pleaded in paragraphs 8(a) and 8(b)(i) above, it was necessary for FIIG to have in place cybersecurity measures which included (but were not limited to) the following:

(a) each of:

(i) a cyber incident response plan which:

(A) identified the action to be taken by the organisation 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;

(ii) management of access to accounts on FIIG's networks, computer systems and applications, relevantly including:

(A) to ensure that:

(I) separate administrative accounts (**Privileged Accounts**) were used for privileged access and tasks, and Privileged Accounts were not used for non-privileged activities;

(II) Privileged Accounts were subject to longer password requirements than those for non-privileged accounts, and passwords for Privileged Accounts were not stored using insecure methods; and

(B) a quarterly review of access rights to ensure that they were appropriate to the status and role of users;

(iii) vulnerability scanning:

(A) involving at least one of the following tool(s):

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

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

(B) involving processes by which:

(I) the tool(s) were run on at least a quarterly basis; and

(II) the results of the scans were reviewed and appropriate action taken to address vulnerabilities;

(iv) penetration testing:

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

(B) in addition, of 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 in subparagraph (I) or (II) occurs;

(v) "next-generation" firewalls configured to impose outbound traffic rules for endpoints and servers, relevantly including rules:

(A) preventing endpoints and servers from establishing direct connections to file transfer protocol (**FTP**) servers over the internet;

(B) preventing internal systems from accessing the internet (except to the extent necessary to perform their role within the business); and

(C) where access to the internet is necessary, limiting the protocols which may be used to connect to the internet;

(vi) configuration of group policies on the Active Directory to disable legacy and insecure authentication protocols, relevantly including Server Message Blocker version 1 (**SMBv1**) and New Technology LAN (Local Area Network) Manger version 1 (**NTLMv1**) hash authentication, in respect of all endpoints and servers;

(vii) Endpoint Detection and Response (**EDR**) software which:

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

(B) was updated regularly as pleaded in subparagraph (viii)(B) below;

(C) generated alerts and logs which were monitored on a daily basis (through Security Incident Events Management (**SIEM**) software referred to in subparagraph (x) below or, alternatively, directly) by a person with sufficient skills, training and experience to identify and respond to any unusual network activity;

(D) was tuned to suppress alerts generated by activities which were known to be non-threatening;

(viii) in respect of patching and software updates:

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

(B) updating EDR software so that:

(I) all EDR software installed on endpoints and servers (**Agents**) were no more than two versions behind the current version of the software, unless there was a known defect with the subsequent version(s); and

(II) all threat signatures were updated at least daily;

(C) updating operating systems and applications so that:

(I) operating systems and applications were sufficiently up to date to be supported by the vendor, unless it was necessary for outdated software to remain in place; and

(II) if and insofar as it was necessary for outdated software for operating systems and applications to remain in place, additional compensating controls were applied to control the increased risk of compromise;

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

(I) four weeks 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; and

(III) 12 months for all other patches;

(ix) from in or about late 2022, multi-factor authentication for all remote access users;

(x) 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 subparagraphs (v), (vi) and (vii) above (**Logs**), to a central location;

(B) undertake analysis of the Logs to identify suspicious activity; and

(C) store the Logs online for at least 90 days, and in an archive for at least twelve months;

(xi) a practice of monitoring of the SIEM, or alternatively the Logs directly, on a daily basis by IT personnel who had the knowledge, skills, experience and capacity to identify and respond to any unusual activity;

(xii) mandatory security awareness training delivered to all employees upon starting, and thereafter annually, addressing the organisation's key cybersecurity risks and the behaviour expected of employees; and

(xiii) 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;

(II) an annual basis for all other controls; and

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

(b) alternatively, such of the measures pleaded in subparagraph (a) above as were necessary for FIIG to adequately protect its clients from the risks and consequences of a cyber attack pleaded in paragraphs 8(a) and 8(b)(i) above,

(**Adequate Cybersecurity Measures**).

Particulars

The need for the Adequate Cybersecurity Measures is informed by:

1. the nature of FIIG's business as pleaded at paragraphs 3 to 6 above;
2. the nature and extent of the information held by FIIG as pleaded at paragraph 5 above;

3. the significant value of the funds under advice and the assets held by FIIG (and on behalf of FIIG and its clients) as pleaded in paragraph 7 above;
4. the Cybersecurity Risks pleaded in paragraph 8 above; and
5. FIIG's contractual obligations pleaded in paragraph 10 above.

ASIC will also rely on expert evidence.

Further particulars may be provided following interlocutory steps.

14. During the Relevant Period, FIIG did not have in place the Adequate Cybersecurity Measures, or alternatively at least some of them, in that:

(a) in respect of a cyber incident response plan (pleaded in paragraph 13(a)(i) above), FIIG did not, in the period from 13 March 2019 to around January 2023:

(i) have a cyber incident response plan addressing the matters pleaded in paragraph 13(a)(i)(A) and 13(a)(i)(B) above; or

(ii) test its cyber incident response plan;

(b) in respect of management of access (pleaded in paragraph 13(a)(ii) above):

(i) 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 subject to longer password requirements than those intended to be used only for non-privileged accounts; and

Particulars to subparagraphs (A) and (B)

The relevant FIIG user accounts were the accounts named "FIIG.local/murrayn" and "FIIG.local/Charles.Anderson".

Further particulars may be provided following interlocutory steps.

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

(ii) throughout the Relevant Period, FIIG did not review access rights to ensure that they were appropriate on a quarterly basis;

(c) in respect of vulnerability scanning (pleaded in paragraph 13(a)(iii) above), FIIG did not, at any time:

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

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

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

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

(d) in respect of penetration testing (pleaded in paragraph 13(a)(iv) above), FIIG:

(i) 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; however

(ii) at all times, did not carry out:

(A) annual external penetration testing in accordance with paragraph 13(a)(iv)(A) above; or

(B) additional penetration testing in accordance with paragraph 13(a)(iv)(B) above;

(e) in respect of "next-generation" firewalls (pleaded in paragraph 13(a)(v) above):

(i) FIIG had Palo Alto "next generation" firewalls (**FIIG's Firewalls**) in place at all times during the Relevant Period; however

(ii) at all times, FIIG's Firewalls were not configured to:

(A) prevent endpoints or servers from establishing direct connections to FTP 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; and

(iii) at all times, 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;

(f) in respect of group policies on Active Directory (pleaded in paragraph 13(a)(vi) above), between 13 March 2019 and at earliest 13 February 2023, FIIG did not configure group policies on the Active Directory to disable insecure SMBv1 and NTLMv1 hash authentication on all endpoints and servers;

(g) in respect of EDR software (pleaded in paragraph 13(a)(vii) above), FIIG:

(i) from in or about July 2019, had installed EDR software "Carbon Black" on some, but not all, of its endpoints and servers;

(ii) at all times, or alternatively between about May 2022 and May 2023:

(A) had Carbon Black Agents which were more than two versions behind the current version of 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;

(iii) at all times, or alternatively from about January 2020 to 8 June 2023, did not:

(A) monitor the logs produced by Carbon Black on a daily basis (either directly or through SIEM software);

(B) further or alternatively, monitor or arrange for monitoring of the Carbon Black logs on a daily basis by a person with sufficient skills, training and experience to identify and respond to any unusual network activity; and

(iv) at all times, did not tune Carbon Black to suppress alerts generated by activities which were known to be non-threatening;

(h) in respect of patching and software updates (pleaded in paragraph 13(a)(viii) above):

(i) FIIG did not at any time, or alternatively did not between 13 March 2019 and at least 13 February 2023:

(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 the time periods pleaded in paragraph 13(a)(viii)(B) above;

(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;

(ii) between 13 March 2019 and at least 13 February 2023, FIIG failed to apply a security patch (released in March 2017) to correct the security vulnerability known as "EternalBlue"; and

(iii) between 14 May 2019 and at least 29 May 2023, FIIG failed to apply a security patch (released in May 2019) to correct the security vulnerability known as "Blue Keep";

(i) in respect of multi-factor authentication (pleaded in paragraph 13(a)(ix) above), FIIG did not, from late 2022, have multi-factor authentication for any of its remote access users;

(j) in respect of SIEM software (pleaded in paragraph 13(a)(x) above), FIIG did not have SIEM software on its network at any time;

(k) in respect of monitoring (pleaded in paragraph 13(a)(xi) above), FIIG did not at any time, or alternatively from about January 2020 to 8 June 2023, have a process in place requiring:

(i) the Logs to be reviewed on a daily basis, either manually or with the assistance of SIEM software, by IT personnel who had the knowledge, skills, experience and capacity to identify and respond to any unusual activity; and

(ii) the Logs to be stored in a secure, centralised location;

(l) in respect of security awareness training (pleaded in paragraph 13(a)(xii) above):

(i) 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 Mr John Prickett to all FIIG employees in 2022 concerning phishing or "spam" emails;

Particulars

Emails from John Prickett to "Allusers" (allusers@fiig.com.au) dated 30 June 2022 [FSL.0012.0002.0440] and 6 October 2022 [FSL.0013.0001.0268].

(ii) FIIG did not at any time:

(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 ensuring that training of the kind pleaded in paragraph 13(a)(xii) above and 14(l)(ii)(A) above occurred on an annual basis; and

(m) in respect of review and evaluation of existing technical controls (pleaded in paragraph 13(a)(xiii) above), FIIG did not, at any time, have a process or processes to review and evaluate:

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

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

(B) an annual basis for all other controls; and

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

Failure to provide financial services efficiently, honestly and fairly

15. By reason of the matters pleaded in paragraphs 12 to 14 above, during the Relevant Period, FIIG did not do all things necessary to ensure that the financial services covered

by the Licence were provided efficiently, honestly and fairly, and so contravened s 912A(1)(a) of the Act.

FIIG's failure to have available adequate resources

Technological resources

16. During the Relevant Period, to have available adequate technological resources to provide the financial services covered by the Licence, FIIG needed to:

    (a) have the Adequate Cybersecurity Measures;

    (b) further or alternatively, have the technological resources necessary to comply with its legal obligations, relevantly including its obligations under ss 912A(1)(a) and 912A(1)(h) of the Act.

17. By reason of:

    (a) the matters pleaded in paragraphs 12 to 14 and 16(a) above;

    (b) further or alternatively, the matters pleaded in paragraphs 12 to 15 and 16(b) above; and

    (c) further or alternatively, the matters pleaded in paragraphs 16(b) above and 26 to 34 below,

    during the Relevant Period, FIIG did not have available adequate technological resources to provide the financial services covered by the Licence.

Human resources

18. During the Relevant Period, to have available adequate human resources to provide the financial services covered by the Licence, FIIG needed available human resources (either within the organisation, or outsourced from a third party) with the skills, available time and responsibility necessary for FIIG to:

    (a) have the Adequate Cybersecurity Measures;

    (b) further or alternatively, implement the cybersecurity measures identified and established by FIIG as part of its risk management system as set out in paragraph 29 below; and

(c) further or alternatively, ensure that it complied with its legal obligations, relevantly including its obligations under ss 912A(1)(a) and 912A(1)(h) of the Act.

19. During the Relevant Period, in order to perform the tasks identified in paragraph 18 above, FIIG needed to:

(a) employ, or outsource from a third party, one or more persons:

(i) with the skills, knowledge and experience in IT security necessary to ensure that FIIG had in place the Adequate Cybersecurity Measures;

(ii) responsible for ensuring that the Adequate Cybersecurity Measures were in place; and

(iii) whose other responsibilities allowed the person/s sufficient time to discharge that responsibility;

(b) further or alternatively, employ, or outsource from a third party, one or more persons:

(i) with the skills, knowledge and experience to implement, or ensure the implementation of, the cybersecurity measures identified and established by FIIG as part of its risk management system; and

(ii) whose other responsibilities allowed the person/s sufficient time to discharge that responsibility; and

(c) employ, or outsource from a third party, sufficient other personnel to ensure that the person/s referred to at subparagraphs (a) and (b) above had time to perform those roles adequately.

20. During the Relevant Period, or alternatively from January 2020 to 8 June 2023, FIIG did not employ or outsource the person/s described in paragraph 19 above.

Particulars

Throughout the Relevant Period, or alternatively from January 2020 to 8 June 2023, FIIG delegated operational responsibility for its IT security to:

(a) its Chief Operating Officer: (i) who was not an expert in IT or IT security; and (ii) for whom IT was one of several areas of responsibility; and

(b) an IT infrastructure team, whose members: (i) had general expertise in IT but had limited expertise in IT security; and (ii) were primarily responsible for IT matters other than IT security.

Further, this is to be inferred from the matters pleaded at paragraphs 12 to 14 above and 29 to 33 below.

Further particulars may be provided following interlocutory steps.

21. By reason of the matters pleaded in paragraphs 18 to 20 above, during the Relevant Period, FIIG did not have available adequate human resources to provide the financial services covered by the Licence.

Financial resources

22. During the Relevant Period, to have available adequate financial resources to provide the financial services covered by the Licence, FIIG needed to provision sufficient financial resources to enable it to:

(a) have the Adequate Cybersecurity Measures;

(b) further or alternatively, put in place the human resources identified in paragraphs 18 and 19 above; and

(c) further or alternatively, ensure that it complied with its legal obligations, relevantly including its obligations under ss 912A(1)(a) and 912A(1)(h) of the Act.

23. During the Relevant Period, FIIG did not provision the funds necessary to:

(a) ensure that it had in place the Adequate Cybersecurity Measures;

(b) employ or outsource the human resources pleaded in paragraphs 18 and 19 above; and/or

(c) comply with its obligations under ss 912A(1)(a) and 912A(1)(h) of the Act.

Particulars to subparagraph (c)

ASIC relies upon the matters pleaded in paragraphs 12 to 15 above and 26 to 34 below.

24. By reason of the matters pleaded in paragraph 22 and 23 above, during the Relevant Period, FIIG did not have available adequate financial resources to provide the financial services covered by the Licence.

25. By reason of one or more of the matters pleaded in:

    (a) paragraph 17 above;

    (b) paragraphs 18 to 21 above; and

    (c) paragraphs 22 to 24 above,

    during the Relevant Period, FIIG contravened s 912A(1)(d) of the Act.

Failure to have adequate risk management systems

26. At all material times, in order to have an adequate risk management system within the meaning of s 912A(1)(h) of the Act, FIIG was required to:

    (a) identify and evaluate risks faced by it and its clients, including the Cybersecurity Risks;

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

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

Failure to mitigate risk using Adequate Cybersecurity Measures

27. During the Relevant Period, by failing to put in place and maintain the Adequate Cybersecurity Measures, FIIG failed to establish and maintain controls adequate to manage or mitigate the Cybersecurity Risks.

Particulars

ASIC repeats the particulars to paragraph 14 above.

28. By reason of the matters pleaded in paragraphs 26 to 27 above, during the Relevant Period, FIIG:

    (a) did not have an adequate risk management system; and so

    (b) contravened s 912A(1)(h) of the Act.

Failure to properly implement controls

FIIG's purported controls

29. During the Relevant Period, the policies and procedures that FIIG put in place to manage the risks it faced in respect of cybersecurity included:

    (a) an **IT Information Security Policy**; and

    (b) a **Cyber and Information Security Policy**.

30. During the Relevant Period, FIIG required:

    (a) between 13 March 2019 and 7 July 2019, under its IT Information Security Policy; and

    (b) from 5 July 2019 to the end of the Relevant Period, under its Cyber and Information Security Policy,

    that:

    (c) accounts with operating system administrative privileges must not be used for day-to-day activities such as email, internet browsing and application access;

    (d) regular penetration or vulnerability tests of FIIG's perimeter must be performed from both internal and external points;

    (e) 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; and

    (f) all event logs must be reviewed by a Security Administrator at least every 90 days.

31. During the Relevant Period, the controls that FIIG identified and established to manage the risks it faced in respect of cybersecurity included the following controls identified in its annual audits of its custodial services (**GS007 Controls**):

    (a) in relation to the financial year ending 30 June 2019:

        (i) monitoring of the network firewall was to be performed on a continual basis;

(ii) FIIG senior technology staff members were to receive an automatic alert about network incidents from the firewall; and

(iii) any incidents were to be automatically alerted to technology staff via email; and

Particulars

GS 007 Type 2 Report on Controls over Custody relating to the period 1 July 2018 to 30 June 2019 [FSL.0035.0001.0140].

(b) in relation to the financial years ending 30 June 2021, 30 June 2022 and 30 June 2023:

(i) the controls described at subparagraph (a) above;

(ii) monitoring and identification of intrusions into the network;

(iii) evaluation of threats by FIIG IT staff to determine the impact of an intrusion; and

(iv) if an intrusion was deemed to have evaded firewall protections and was exploiting a vulnerability relevant to the technology being attacked, undertaking of further investigation and remediation.

Particulars

GS 007 Type 2 Report on Controls over Custody relating to the period 1 July 2020 to 30 June 2021 [FSL.0034.0001.0018].

GS 007 Type 2 Report on Controls over Custody relating to the period 1 July 2021 to 30 June 2022 [FSL.0014.0001.0635].

GS 007 Type 2 Report on Controls over Custody relating to the period 1 July 2022 to 30 June 2023 [FSL.0034.0001.2628].

FIIG's implementation of its purported controls

32. During the Relevant Period, FIIG did not implement the controls identified and established in its IT Information Security Policy and Cyber and Information Security Policy as pleaded at paragraph 30 above, in that:

(a) from 13 March 2019 until at least 13 February 2023, FIIG user accounts:

(i) had operating system administrative privileges; and

(ii) were used for day-to-day activities such as email and internet browsing;

Particulars

The user accounts “FIIG.local/murrayn” and “FIIG.local/Charles.Anderson”.

(b) throughout the Relevant Period, FIIG did not install the most recent operating system or application security patches;

(c) throughout the Relevant Period, FIIG did not review all event logs at least every 90 days; and

(d) between 13 March 2019 and about January 2023, no penetration or vulnerability testing was performed on FIIG’s network.

33. Between about January 2020 and 8 June 2023, FIIG did not implement, or alternatively fully implement, the GS007 Controls, in that the network firewall in respect of FIIG’s Sydney and Melbourne offices (the **Sydney Firewall**) did not send automatic alerts about network incidents that were threats to FIIG senior technology staff members.

34. By reason of the matters pleaded in paragraphs 29 to 33 above, during the Relevant Period, FIIG:

(a) failed to implement the controls identified and adopted under its risk management system, or alternatively failed to implement those controls properly or to the extent required by that system;

(b) thus did not have adequate risk management systems; and so

(c) contravened s 912A(1)(h) of the Act.

Further failures to provide services "efficiently, honestly and fairly"

35. By reason of one or more of:

(a) the matters pleaded in paragraphs 18 to 25 above; and

(b) the matters pleaded in paragraphs 26 to 34 above,

FIIG did not do all things necessary to ensure that the financial services covered by the Licence were provided efficiently, honestly and fairly, and so contravened s 912A(1)(a) of the Act.

Contraventions of civil penalty provisions

36. By reason of one or more of:

    (a) the matters pleaded in paragraph 15 above;

    (b) the matters pleaded in paragraph 25 above;

    (c) the matters pleaded in paragraph 28 above;

    (d) the matters pleaded in paragraph 34 above; and

    (e) the matters pleaded in paragraph 35 above,

    FIIG contravened s 912A(5A) of the Act.

FIIG's data breach

37. On 19 May 2023, a FIIG employee used a laptop issued by FIIG to download a .zip file from the internet.

38. The .zip file contained a JavaScript file named “second ranking general security agreement 85822.js” (the **Malware**), which invoked the JavaScript file handler program “wscript.exe”.

39. The employee unwittingly opened the Malware, which:

    (a) downloaded additional, second stage JavaScript malware “Queue Management.js”; and

    (b) created a scheduled task to execute the second stage malware.

40. The second stage malware, when executed, allowed one or more unknown persons to:

    (a) remotely access FIIG’s network and perform network-based lateral movement and privilege escalation;

    (b) on 19 May 2023, obtain access to a standard user account on FIIG’s network;

    (c) on or about 20 May 2023, obtain access to a domain account on FIIG’s network;

(d) on or about 22 May 2023, obtain access to one of FIIG's database servers;

(e) on or about 23 May 2023, obtain access to a privileged user account on FIIG's network; and

(f) between about 23 May 2023 and 30 May 2023, use the program FreeFileSync to download approximately 385 GB of data held on FIIG's file servers, including Personal Client Information, to an external site.

41. From 23 May 2023 to 3 June 2024:

(a) email alerts and daily reports were generated by FIIG's Brisbane firewall and sent to FIIG's IT Infrastructure team; and

(b) those alerts and reports identified threats related to FTP activity between FIIG's file servers and the external site referred to in paragraph 40(f) above.

42. Prior to 2 June 2023, and despite the matters in paragraph 41 above, FIIG had not identified or responded to the cyber intrusion described at paragraph 40 above.

43. On 2 June 2023, the Australian Cyber Security Centre (**ACSC**):

(a) informed FIIG to the effect that an account or device on its network may have been compromised;

Particulars

Telephone call between Mr Murray Nicolls of FIIG and a representative of the ACSC following a voicemail message left by the ACSC on 1 June 2023 and a follow-up call from the ACSC to FIIG on 2 June 2023.

(b) informed FIIG that it had received "a report from a trusted third party of potentially malicious activity being identified on [FIIG's] network";

(c) provided FIIG with details of the computer and account suspected to be compromised; and

(d) recommended that FIIG investigate the issue.

Particulars

Email from the ACSC to Mr Nicolls' personal email address dated 2 June 2023 at 10.19pm [FSL.0020.0001.0486].

44. On 8 June 2023, FIIG:

    (a) inspected the laptop;

    (b) identified that it had been used to access multiple user accounts, including a privileged user account; and

    (c) engaged external cybersecurity consultants to undertake a forensic investigation.

45. On or about 8 June 2023, FIIG's external cybersecurity consultants identified that:

    (a) the laptop and FIIG user accounts had been compromised; and

    (b) an unknown person had accessed data on FIIG's servers and downloaded data to an external site.

46. On or about 9 June 2023, FIIG took its systems offline.

47. On or about 10 June 2023, an unknown person published screenshots of two documents containing Personal Client Information, which had been downloaded during the data breach described at paras 39, 40 and 45 above, on the dark web.

48. If, as at 19 May 2023, FIIG had:

    (a) had in place the Adequate Cybersecurity Measures;

    (b) further or alternatively, complied with the policies and procedures it had put in place to manage the risk it faced in respect of cybersecurity (including those in paragraphs 29 and 31 above),

    then, in the event of the download of the .zip file containing the Malware and opening of the Malware, FIIG would have:

    (c) detected suspicious activity on its network on or shortly after 19 May 2023 or, alternatively, by on or about 22 May 2023;

    (d) implemented its cyber incident response plan on or shortly after 19 May 2023 or, alternatively, by on or about 22 May 2023;

    (e) identified the presence of a threat actor within its system before 23 May 2023 or, alternatively, before 30 May 2023; and

    (f) prevented all or alternatively some of the Personal Client Information from being downloaded from FIIG's servers.

49. In the premises of paragraph 48 above, the loss of control over the data pleaded in paragraphs 40(f) and 45 above occurred because of FIIG's contraventions of s 912A(1)(a), further or alternatively s 912A(1)(d), further or alternatively s 912A(1)(h).

Relief

By reason of the matters referred to above, ASIC seeks the following relief

Declarations

1. A declaration pursuant to s 1317E of the Act that, at all times during the period between 13 March 2019 and 8 June 2023 (or such part of that period as the Court determines), FIIG failed to:

    (a) have available the technological resources:

        (i) comprising the Adequate Cybersecurity Measures; and

        (ii) further or alternatively, necessary to comply with its legal obligations;

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

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

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

        (iii) further or alternatively, ensure that it complied with its legal obligations;

    (c) further or alternatively, provision sufficient financial resources to enable FIIG to:

        (i) have in place the Adequate Cybersecurity Measures; and

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

            (A) have in place the Adequate Cybersecurity Measures;

            (B) further or alternatively, implement the controls identified and established as part of its risk management system to mitigate the cybersecurity risks it faced;

(C) further or alternatively, 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 Licence in contravention of s 912A(1)(d) and s 912A(5A) of the Act.

2. Declarations pursuant to s 1317E of the Act that:

(a) at all times during the period between 13 March 2019 and 8 June 2023 (or such part of that period as the Court determines), FIIG failed to have in place the Adequate Cybersecurity Measures and thereby failed to have adequate risk management systems in contravention of s 912A(1)(h) and s 912A(5A) of the Act; and

(b) at all times between 13 March 2019 and 8 June 2023 (or alternatively such part of that period as the Court determines), 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 in contravention of s 912A(1)(h) and s 912A(5A) of the Act.

3. A declaration pursuant to s 1317E of the Act that, at all times during the period between 13 March 2019 and 8 June 2023 (or such part of that period as the Court determines), by reason of one or more of FIIG's failures to:

(a) have in place the Adequate Cybersecurity Measures;

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

(c) further or alternatively, have adequate risk management systems,

FIIG failed to do all things necessary to ensure that the financial services covered by its Licence were provided efficiently, honestly and fairly in contravention of s 912A(1)(a) and s 912A(5A) of the Act.

Pecuniary penalties

4. An order pursuant to s 1317G of the Act that FIIG pay to the Commonwealth of Australia such pecuniary penalties as the Court considers appropriate in respect of each of FIIG's contraventions of s 912A(5A) identified in paragraphs 1, 2 and 3 above.

Compliance order

5. An order under s 1101B of the Act that the defendant complete a compliance programme at its cost involving:

   (a) review of its cybersecurity measures;

   (b) commissioning of an independent expert to report on those measures;

   (c) actioning of all reasonable recommendations of the independent expert; and

   (d) reporting to ASIC about the matters referred to in subparagraphs (a) to (c) above,

   in such form as the court thinks fit.

Other orders

6. An order that FIIG pay ASIC's costs.

7. Such further or other order as the Court considers appropriate.

Date: 26 May 2025

Signed by Melinda Smith
Lawyer for the Applicant

This pleading was prepared by Stewart Maiden KC, Angus O'Brien and Mei Ying Barnes of Counsel.

Certificate of lawyer

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

Date: 26 May 2025

Signed by Melinda Smith
Lawyer for the Applicant