Filed: 21 July 2025 3:20 PM

D00026VWC8

Form 2

ORIGINATING PROCESS – COVERSHEET AND ACKNOWLEDGEMENT

IN THE MATTER OF FORTNUM PRIVATE WEALTH LTD

COURT DETAILS

Court	Supreme Court of NSW
Division	Equity
List	Corporations List
Registry	Supreme Court Sydney
Case number	2025/00278865

TITLE OF PROCEEDINGS

First Plaintiff	AUSTRALIAN SECURITIES & INVESTMENTS COMMISSION ABN 86768265615
First Defendant	FORTNUM PRIVATE WEALTH LTD ACN 139889535

FILING DETAILS

Filed for	AUSTRALIAN SECURITIES & INVESTMENTS COMMISSION, Plaintiff 1
Legal representative	Rayma Gupta
Legal representative reference	
Telephone	[redacted]
Your reference	CAS-123881-Q8J2D0

HEARING DETAILS

This application will be heard at Supreme Court Sydney on 4 August 2025 at 10:00 AM

ATTACHMENT DETAILS

In accordance with Part 3 of the UCPR, this coversheet confirms that both the Originating process (Corporations Law) Other, along with any other documents listed below, were filed by the Court.

Corporations Law Originating Process (Form 2) (20250721 ASIC v Fortnum Originating Process.pdf)
Other supporting documents (e.g. Affidavit of Search/Authority to Act) (20250721 ASIC v Fortnum Concise Statement.pdf)

[attach.]

Form 2
(rules 2.2 and 15A.3)

IN THE SUPREME COURT OF NEW SOUTH WALES No. of 2025
DIVISON: EQUITY
LIST: CORPORATIONS
REGISTRY: SYDNEY

IN THE MATTER OF FORTNUM PRIVATE WEALTH LIMITED
ACN: 139 889 535

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION
Plaintiff

FORTNUM PRIVATE WEALTH LIMITED ACN 139 889 535
Defendant

ORIGINATING PROCESS

A. DETAILS OF APPLICATION

This application is made under sections 1317E(1), 1317G(1) and 1317J(1) of the *Corporations Act 2001* (Cth) (**Corporations Act**). This proceeding concerns contraventions by the defendant of its statutory obligations as a financial services licensee under the Corporations Act.

On the facts stated in the plaintiff's concise statement, the plaintiff seeks the following orders:

1. A declaration pursuant to s 1317E(1) of the Corporations Act that, in the period from 20 April 2021 to 11 May 2023, Fortnum Private Wealth Limited (**Fortnum**):

    a. did not do all things necessary to ensure that the financial services covered by its Australian financial services licence (**the Licence**)

were provided efficiently, honestly and fairly, and thereby contravened ss 912A(1)(a) and 912A(5A) of the Corporations Act, by its failure to:

i. implement any adequate cybersecurity policy to manage and mitigate cybersecurity risks for it and its authorised representatives (**ARs**);

ii. provide any adequate education or training its ARs on cybersecurity; and

iii. implement any, or any adequate, processes, systems or frameworks for the oversight and monitoring of its ARs in terms of cybersecurity risk and cyber resilience;

b. failed to have available adequate resources (specifically human resources) to provide the financial services covered by the Licence and to carry out supervisory arrangements, and thereby contravened ss 912A(1)(d) and 912A(5A) of the Corporations Act;

c. failed to ensure that its ARs were adequately trained, and were competent to, provide the financial services covered by the Licence, and thereby contravened ss 912A(1)(f) and 912A(5A) of the Corporations Act; and

d. failed to have adequate risk management systems, and thereby contravened ss 912A(1)(h) and 912A(5A) of the Corporations Act.

2. An order pursuant to s 1317G(1) of the Corporations Act that Fortnum pay to the Commonwealth a pecuniary penalty or penalties in respect of the contraventions referred to in paragraph 1 above in such amount as the Court considers appropriate.

3. An order that the defendant pay the plaintiff's costs of and incidental to this proceeding.

4. Such other orders as the Court sees fit.

Date: 21 July 2025

.....

Rayma Gupta
Solicitor for the
Australian Securities and Investments
Commission

This application will be heard by the Supreme Court of New South Wales at Law Courts Building, Queens Square, 184 Phillip Street, Sydney NSW at
am/pm on

B. NOTICE TO DEFENDANT

TO: **FORTNUM PRIVATE WEALTH LIMITED** of Level 6, 88 Phillip Street, Sydney, New South Wales 2000

If you or your legal practitioner do not appear before the Court at the time shown above, the application may be dealt with, and an order made, in your absence. As soon after that time as the business of the Court will allow, any of the following may happen:

(a) the application may be heard and final relief given;
(b) directions may be given for the future conduct of the proceeding;
(c) any interlocutory application may be heard.

Before appearing before the Court, you must file a notice of appearance, in the prescribed form, in the Registry and serve a copy of it on the plaintiff.

Note.

Unless the Court otherwise orders, a defendant that is a corporation must be represented at a hearing by a legal practitioner. It may be represented at a hearing by a director of the corporation only if the Court grants leave.

C. FILING

Date of filing: 21 July 2025

This originating process is filed by Rayma Gupta, Legal Practitioner for the plaintiff, Australian Securities and Investments Commission.

D. SERVICE

The plaintiff's address for service is:

Australian Securities and Investments Commission
Level 5, 100 Market Street
Sydney NSW 2000
Attention: Rayma Gupta/ Robert MacAlpine

It is intended to serve a copy of this originating process on the defendant.

IN THE SUPREME COURT OF NEW SOUTH WALES No. of 2025
DIVISON: EQUITY
LIST: CORPORATIONS
REGISTRY: SYDNEY
IN THE MATTER OF FORTNUM PRIVATE WEALTH LIMITED
ACN: 139 889 535

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION
Plaintiff

FORTNUM PRIVATE WEALTH LIMITED ACN 139 889 535
Defendant

CONCISE STATEMENT

A. INTRODUCTION

1. The defendant, Fortnum Private Wealth Ltd (**Fortnum**), is a financial services licensee. It holds an Australian financial services licence (**AFSL**) which authorises it to, among other things, provide financial product advice (within the meaning of s 766B of the *Corporations Act 2001* (Cth) (**Corporations Act**)).

2. At all material times, Fortnum had a number of authorised representatives (**ARs**), which included firms who operated financial advice businesses (**Principal Practices**) and individual advisers employed by the Principal Practices (**Authorised Advisers**). Fortnum's ARs provided financial product advice, including personal advice (within the meaning of s 766B of the Corporations Act) (**Personal Advice**) to retail clients (within the meaning of s 761G of the Corporations Act) (**Retail Clients**) on Fortnum's behalf.

3. This proceeding concerns contraventions by Fortnum of its statutory obligations as a financial services licensee under the Corporations Act.

B. THE IMPORTANT FACTS GIVING RISE TO THE CLAIM

Cybersecurity risks

4. In the course of their business, Fortnum's ARs electronically received, stored and accessed confidential and sensitive personal information and documents in relation to Retail Clients, including (among other things) copies of identification documents, tax file numbers, and financial information such as bank account and credit card details (**Personal Information**).

5. It was necessary for the clients of Fortnum's ARs to provide their Personal Information in order to receive Personal Advice.

6. As a result of the nature and extent of the Personal Information collected and held in the course of providing financial services, Fortnum and each of its ARs were potential targets for cyber-related attacks and cybercrimes, the consequences of which could include serious harm and loss.

7. It therefore was, and is, incumbent on Fortnum in discharging its duties and obligations as a licensee to identify and understand the cybersecurity risks that it and its ARs faced, and to have adequate policies, frameworks, systems and controls in place to appropriately manage and mitigate those risks.

Fortnum's cybersecurity policies

8. Despite the risk of cyber-related attacks and cybercrimes, prior to 11 May 2023, Fortnum did not have any adequate policies in place which were designed to manage and mitigate the cybersecurity risks faced by it or its ARs.

9. On 20 April 2021, Fortnum issued a policy to its ARs entitled "Cyber Security Policy Version 1.0" (**April 2021 Policy**). The April 2021 Policy was the first policy implemented by Fortnum which was specifically directed at cybersecurity.

10. The April 2021 Policy required that all Principal Practices take certain steps in respect of cybersecurity. Among other things, pursuant to the policy:

    a. by 1 September 2021, Fortnum's Principal Practices were required to:

        i. complete a self-assessment tool, which involved a series of questions regarding the Principal Practices' cybersecurity and IT set-up with the available responses being "yes", "no", or "unsure" (**Self-Assessment**);

ii. engage with either Fortnum or an IT consultant regarding those questions in the Self-Assessment to which the Principal Practice responded "no" or "unsure"; and

iii. complete a form confirming the cybersecurity measures that had been implemented (**Attestation**); and

b. Fortnum was to conduct an annual review in September of each Principal Practices' cybersecurity strategy.

11. However, the April 2021 Policy was not adequate to manage and mitigate the cybersecurity risks faced by Fortnum and its ARs, including because the recommended measures were not specific or stringent enough where, *inter alia*, that policy:

a. did not mandate that Principal Practices consult or otherwise engage with Fortnum where they had responded "no" or "unsure" to any questions in the Self-Assessment;

b. allowed Principal Practices to consult or otherwise engage with a consultant where they had responded "no" or "unsure" to any questions in the Self-Assessment in circumstances where Fortnum had no policies, processes or systems in place to ensure that such consultants had adequate and appropriate experience and expertise;

c. did not mandate that Principal Practices uplift or otherwise change their practices in respect of those questions in the Self-Assessment to which they had responded "no" or "unsure"; and

d. only included mitigation strategies, such as those set out in the Australian Cyber Security Centre's Essential Eight Maturity Model as part of an advanced cyber security strategy which was optional.

12. Further, following its introduction, Fortnum did not take any steps to ensure that its Principal Practices completed the Self-Assessment and the Attestation, as required by the April 2021 Policy. As a result, by 1 September 2021, only approximately 44% of Principal Practices had completed the Self-Assessment, and only approximately 11% of Principal Practices had completed the Attestation.

13. In the period from approximately May to July 2022, Fortnum decided to develop an update to the April 2021 Policy, because it was thought that the minimum requirements under the April 2021 Policy were not stringent enough. At around the same time, because an update was being developed, Fortnum decided not to require its Principal Practices to complete the Self-Assessment or the Attestation and not to pursue the annual review, as required by the April 2021 Policy.

14. However, the policy update was ultimately not introduced until approximately a year later, on 11 May 2023, when Fortnum issued a policy to its ARs entitled "Cyber Policy Version 2.1" (**May 2023 Policy**). During that 12 month period during which the May 2023 Policy was being developed, Fortnum did not take any steps to implement interim measures above and beyond the April 2021 Policy.

Fortnum's cybersecurity practices more broadly

15. Aside from the April 2021 Policy, there were other aspects of Fortnum's policies, frameworks, systems and controls which should have, but did not, address cybersecurity risks.

16. *First*, Fortnum had a statutory obligation under the Corporations Act as a financial licensee, and a contractual obligation arising under its agreement with its ARs, to provide its ARs with education and training. However Fortnum did not require that its ARs undertake a prescribed minimum amount of cybersecurity education or training. Further, while Fortnum provided its ARs with five education or training activities related to cyber-security in the period prior to 11 May 2023, all of those were focused on the requirements of the April 2021 Policy or the May 2023 Policy.

17. *Second*, it was incumbent on Fortnum as licensee to ensure that it supervised its ARs' conduct. While Fortnum had in place policies, frameworks, systems and controls for the monitoring and oversight of ARs in certain respects – for example, to monitor the quality of financial advice given by ARs to clients – it did not have anything in place in respect of cybersecurity. For example, Fortnum's frameworks did not enable it to oversee or monitor whether ARs were complying with the April 2021 Policy, or whether any IT or cybersecurity consultants retained by ARs had appropriate expertise and experience.

18. *Third*, Fortnum did not have any employees with specialised expertise or experience in cybersecurity. It also did not engage any cybersecurity consultants with expertise or experience when it would have been appropriate to do so, for example when Fortnum was developing the April 2021 Policy.

19. *Fourth,* Fortnum had a statutory obligation under the Corporations Act as a financial licensee to have in place a risk management system. However Fortnum did not have a risk management system which addressed cybersecurity. In particular, Fortnum did not have any policies, frameworks, systems or controls which: enabled the identification and evaluation of cybersecurity risks across its ARs; were designed to manage and mitigate those risks; documented the roles and responsibilities of Fortnum and its ARs as to the management and mitigation of those risks; and enabled the identification, reporting and escalation of cybersecurity issues by ARs to Fortnum.

Cybersecurity incidents affecting Fortnum's ARs

20. In the period prior to 11 May 2023, several of Fortnum's ARs experienced cybersecurity incidents. Those include:

    a. On or around 26 January 2021, the email address of an Authorised Adviser of one of Fortnum's then Principal Practices, Prominent Financial Services Pty Ltd, was compromised.

    b. In or around late March or April 2021, the email address of an employee of one of Fortnum's Principal Practices, Ford, was hacked and accessed by an overseas IP address.

    c. On or around 1 July 2021, one of Fortnum's Principal Practices, RedThorn, was subject to a cyberattack where emails were sent purporting to be from one of RedThorn's advisers.

    d. On or around 26 July 2022, one of Fortnum's Principal Practices, Eureka, was the subject of a phishing attack which resulted in an unknown threat actor gaining access to at least one employee's email account and sending 1,266 emails containing phishing links from that employee's account.

    e. In the period 5 September 2022 to 20 September 2022, one of Fortnum's Principal Practices, Wealthwise, experienced a major data

breach which resulted in the exfiltration and publication of over 200 gigabytes of data relating to up to 9,828 clients.

21. Most of those incidents occurred *after* the introduction of the April 2021 Policy. Fortnum did not implement any measures in light of those incidents in respect of its cybersecurity policies, frameworks, systems and controls.

C. THE RELIEF SOUGHT FROM THE COURT

22. ASIC seeks a declaration and a pecuniary penalty or penalties against the defendant as set out in the Originating Process.

D. THE PRIMARY LEGAL GROUNDS FOR THE RELIEF SOUGHT

23. By reason of the matters referred to above, and as set out in the Originating Process, Fortnum breached its obligations as a financial services licensee and contravened ss 912A(1)(a), (d), (f) and (h), and (5A), of the Corporations Act.

E. THE HARM SUFFERED

24. By failing to have in place adequate policies, frameworks, systems and controls in respect of cybersecurity risks, Fortnum exposed itself, its ARs and its ARs' clients to an unacceptable level of risk of a cyber-attack or cybersecurity incident, the consequences of which could include serious harm and loss.

This concise statement was prepared by Justin Hewitt SC, Dr Greg O'Mahoney and Emily Hall, counsel, for the Australian Securities and Investments Commission.

Certificate of lawyer

I, Rayma Gupta, 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: 21 July 2025

Signed by Rayma Gupta
Lawyer for the Plaintiff