Federal Court of Australia

District Registry: Victoria

Division: General No: VID429/2024

AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY
Applicant

OPTUS MOBILE PTY LIMITED ACN 054 365 696
Respondent

ORDER

JUDGE: JUSTICE BEACH

DATE OF ORDER: 19 June 2024

WHERE MADE: Melbourne

THE COURT ORDERS THAT:

Concise statement

1. Until further order, pursuant to sections 37AF(1) and 37AG(1)(a) of the *Federal Court of Australia Act 1976* (Cth), the concise statement (without the confidential annexure) filed in this proceeding on 22 May 2024 (Concise Statement) and the confidential annexure to the Concise Statement cannot be disclosed or published until further order.

2. The applicant file and serve a copy of the Concise Statement with redactions applied consistent with the version annexed to these orders by 19 June 2024.

3. The version of the Concise Statement filed and served in accordance with paragraph 2 above may be inspected and published.

Pleadings

4. The applicant file and serve a statement of claim by 19 July 2024.

5. The respondent file and serve a defence by 23 August 2024.

6. The applicant file and serve any reply by 4 September 2024.

Notice to Produce

7. The respondent produce to the applicant a copy of the final report prepared by Deloitte sought by the applicant's notice to produce dated 5 June 2024 (Notice) by 4pm on 21 June 2024.

8. The applicant is bound by the terms of the interim confidentiality regime agreed by the parties in relation to the report produced in accordance with paragraph 7 above until further order.

9. The date for compliance with the Notice is otherwise stood over until 9.30 am on 13 September 2024.

Other orders

10. The matter be listed for a case management hearing at 9.30 am on 13 September 2024.

11. Costs are reserved.

12. Liberty to apply on two (2) days' notice.

Date that entry is stamped: 19 June 2024

Registrar

Annexure

NCF1

CONCISE STATEMENT

FEDERAL COURT OF AUSTRALIA
DISTRICT REGISTRY: VICTORIA
DIVISION: GENERAL **NO VID OF 2024**

AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY
Applicant

OPTUS MOBILE PTY LIMITED ACN 054 365 696
Respondent

A. INTRODUCTION

1. This proceeding concerns a failure by the Respondent (**Optus**) to protect the confidentiality of personally identifiable information of around 3.6 million customers from unauthorised interference or unauthorised access in the period 17 to 20 September 2022 (**Relevant Period**).

2. Optus' failure was due to a coding error which it did not detect during (and for four years prior to) the Relevant Period. As a result, the personally identifiable information of more than 9.5 million former and current customers of **Singtel Optus** Pty Limited and its subsidiaries was accessed by a cyberattacker. That information included full names, dates of birth, phone numbers, residential addresses, drivers licence details and passport and Medicare card numbers. Some customers' information was then published on the dark web.

3. The Applicant (**ACMA**) alleges that Optus' conduct in failing to protect the information from this unauthorised access or unauthorised interference by cyberattack contravened s 187A(1) of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**). The ACMA seeks civil penalties against Optus for its failure to protect the personally identifiable information of at least 3.6 million active customers.

4. Further details of Optus' systems and the cyberattack are identified in the **Confidential Annexure**.

B. IMPORTANT FACTS GIVING RISE TO THE CLAIM

Optus' systems

5. Optus is a subsidiary of Singtel Optus, which offers mobile, landline and internet services and is the second largest telecommunications company in Australia. During

Filed on behalf of the Applicant, Australian Communications and Media Authority
File ref: 23005233
Prepared by: Jody Marshall
AGS lawyer within the meaning of s 55I of the *Judiciary Act 1903*
Telephone: 07 3360 5751
Lawyer's Email: Jody.Marshall@ags.gov.au
Address for Service:
The Australian Government Solicitor,
Level 33, 300 George St, Brisbane, QLD 4000
Jody.Marshall@ags.gov.au

the Relevant Period, Optus provided prepaid and postpaid mobile and mobile broadband services, and fixed services including home broadband.

6. When buying or activating an Optus product, both before and during the Relevant Period, customers were required to provide Optus with their personally identifiable information.

7. During the Relevant Period, Optus kept customers' personally identifiable information on a [redacted]. The [redacted] was a sub-system of a [redacted]. The [redacted] interfaced with downstream applications that held customer information, including the [redacted].

8. Customers could retrieve information from the [redacted] in various ways, including through certain Application Programming Interfaces (**APIs**) accessible from domains including www.optus.com.au (**Main Domain**) and api.www.optus.com.au (**Target Domain**). An API is an interface that allows two or more computer programs to communicate with each other to retrieve and return information. The [redacted] had three APIs that enabled information to be retrieved from the [redacted] after a customer was successfully authenticated (**Target APIs**).

9. The intended use of the Target Domain was to segregate API traffic from static content on the Main Domain, to assist with performance and customer experience on the website. During the Relevant Period, the Target Domain was dormant and not in use, and had not been in use since 2017. Despite this, the Target Domain was not decommissioned until after the cyberattack.

The vulnerabilities

10. The Target Domain was internet facing from 20 April 2017. Access to the Target APIs was secured by various access controls designed to prevent unauthorised access. In September 2018, a **coding error** was made in one of the access controls which caused it to be ineffective for both the Target Domain and Main Domain. This left these domains vulnerable to attack once both domains became internet facing with the coding error in June 2020.

11. In August 2021, Optus detected that the Main Domain was vulnerable to attack due to the coding error. Optus fixed the error for the Main Domain but did not detect or fix that same issue which affected the Target Domain.

12. The coding error was not identified by Optus until after the cyberattack (explained below) had occurred in mid-September 2022. Optus had the opportunity to identify the coding error at several stages in the preceding four years including: when the coding change was released into a production environment following review and testing in September 2018; when the Target Domain (and the Main Domain) became internet facing through the production environment in June 2020; and when the coding error was detected for the Main Domain in August 2021.

13. The Target Domain was permitted to sit dormant and vulnerable to attack for two years and was not decommissioned despite the lack of any need for it.

The cyberattack

14. Between 17 and 20 September 2022, a cyberattacker accessed the [redacted] and obtained customers' personally identifiable information through the Target Domain for around 9.5 million current and former customers of Singtel Optus. By exploiting the coding error, the cyberattacker was able to bypass access controls and send requests to the Target APIs which returned customers' personal identifying information.

15. The cyberattack was not highly sophisticated or one that required advanced skills or proprietary or internal knowledge of Optus' processes or systems. It was carried out through a simple process of trial and error.

16. The cyberattack was first detected on 17 September 2022. Following investigation, Optus became aware that a cyberattack was happening at around 8pm on 19 September 2022 and blocked the internet traffic to the Target Domain at around 3:45am on 20 September 2022. Optus confirmed that the attack involved customer data and informed Optus group executives on 21 September 2022. On 21 September 2022, the Target Domain was decommissioned.

C. SUMMARY OF RELIEF SOUGHT FROM THE COURT

17. The ACMA seeks pecuniary penalties and the other relief set out in the accompanying Originating Application.

D. PRIMARY LEGAL GROUNDS FOR RELIEF SOUGHT

18. During the Relevant Period, s 187A(1) of the TIA Act imposed obligations on a person who operated a service to which Part 5-1A of the TIA Act applied to keep or cause to be kept, in accordance with s 187BA, information of a kind specified in or under s 187AA (or documents containing information of that kind) relating to any communication carried by means of the service.

19. Optus operated the services referred to in paragraph 5 above, which were services to which Part 5-1A of the TIA Act applied.

20. The personally identifiable information provided to Optus was (and/or the documents provided to Optus contained) information of a kind specified under s 187AA(1) of the TIA Act.

21. By reason of the matters in paragraphs 18 to 20 above, during the Relevant Period Optus was obliged by s 187A(1) to keep, or cause to be kept, the personally identifiable information in accordance with s 187BA of the TIA Act.

22. Section 187BA of the TIA Act required Optus to protect the confidentiality of the information that it was obliged to keep, or cause to be kept, by protecting the information from unauthorised interference or unauthorised access.

23. By failing to protect the confidentiality of its customers' information from unauthorised interference or unauthorised access, Optus contravened s 187A(1) of the TIA Act. There were during the Relevant Period at least 3.6 million instances of unauthorised

access to or unauthorised interference with the personally identifiable customer information.

24. Accordingly, Optus during the Relevant Period contravened s 187A(1) of the TIA Act at least 3.6 million times.

25. Section 187A(1) of the TIA Act is a civil penalty provision, each contravention of which carries a maximum penalty of $250,000 (s 570(3)(b) of the *Telecommunications Act 1997* (Cth)).

E. ALLEGED HARM

26. The records of over 9.5 million former and current customers of Singtel Optus (and approximately 36% of the Australian population) were accessed during the cyberattack. Of those, at least 3.6 million were active subscribers of a (mobile) service or services provided by Optus. The ACMA seeks penalties for the contraventions in relation to those (at least 3.6 million) active customers.

27. The cyberattack affected customers differently, as not all categories of personally identifiable information were accessed for all customers. All customers had their full name, email address, date of birth and telephone number accessed. Of the active subscribers of an Optus service, 3,154,171 customers had their physical address accessed and 2,470,036 customers had identity information accessed (for example, passport number, driver's licence number and card number, Medicare card number, or birth certificate information).

28. The cyberattack led to the personally identifiable information of approximately 10,200 Singtel Optus customers being published on the dark web.

29. Singtel Optus has reimbursed 20,071 former and current customers for replacement identity documents (where the cost was not otherwise waived), and has offered certain fraud mitigation protections to customers based on the risk level associated with the types of information accessed. Singtel Optus is also in the process of reimbursing agencies for the costs incurred in replacing identity documents.

CERTIFICATE OF LAWYER

I Jody Maree Marshall 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: 20 May 2024

.....

Jody Marshall
AGS lawyer
for and on behalf of the Australian Government Solicitor
Lawyer for the Applicant

This Concise Statement was prepared by Michael Borsky KC and Jacqueline Fumberger of counsel.