Form NCF1

Concise Statement

No. of

Federal Court of Australia

District Registry: Victoria

Division: General

Commercial and Corporations Practice Area (Regulator and Consumer Protection)

AUSTRALIAN INFORMATION COMMISSIONER

Applicant

MEDIBANK PRIVATE LIMITED ACN 080 890 259

Respondent

A INTRODUCTION

1 The Applicant (**AIC**) alleges that, during the period from 12 March 2021 to 13 October 2022 (**Relevant Period**), the Respondent (**Medibank**) seriously, further or alternatively repeatedly, interfered with the privacy of approximately 9.7 million individuals (comprising current and former Medibank customers), whose personal information it held, in contravention of s 13G of the *Privacy Act 1988* (Cth) (**Act**), by failing to take reasonable steps to protect that personal information from misuse, and/or from unauthorised access or disclosure, in breach of Australian Privacy Principle (**APP**) 11.1.

B IMPORTANT FACTS GIVING RISE TO THE CLAIM

2 Medibank was incorporated on 1 December 1997 and has been listed on the Australian Securities Exchange since 25 November 2014. It is a large private health insurer in Australia, which provides health insurance policies under its own Medibank brand as well as under its 'ahm' and 'ahm health insurance' brands. For the financial years ending 30 June 2021, 2022, and 2023, Medibank generated revenue of approximately $6.9 billion, $7.1 billion, and $7.1 billion and annual profit before tax of $632.3 million, $560 million, and $727.1 million, respectively. As at 30 June 2022, Medibank employed approximately 3,291 full time employees.

3 Medibank collects and holds individual customers' personal information and health information in the context of a business directed towards providing health insurance services. During the Relevant Period, the personal information collected and held by Medibank included names, dates of birth, home addresses, phone numbers, email addresses, employment details, passport numbers, Medicare numbers, financial information, and sensitive information within the meaning of s 6 of the Act. The personal information included sensitive information about Medibank's customers' race and ethnicity and health information such as information about any illnesses, disabilities or injuries, health services provided to the individual and health claims data. During the Relevant Period Medibank was, and remains, an APP entity within the meaning of s 6 of the Act and was, and is, required to comply with the APPs in its handling of personal information.

Filed on behalf of (name & role of party) Australian Information Commissioner, Applicant
Prepared by (name of person/lawyer) Gowri Kangeson
Law firm (if applicable) DLA Piper Australia
Tel (03) 9274 5428 Fax
Email gowri.kangeson@dlapiper.com
Address for service (include state and postcode) Level 14, 80 Collins Street, Melbourne VIC 3000

Medibank's cybersecurity and information security framework

4 APP 11.1 required Medibank to take such steps, as were reasonable in the circumstances, to protect the personal information it held from: (a) misuse, interference, and loss; and (b) unauthorised access, modification or disclosure. The content of the obligation which APP 11.1 imposes will vary according to the particular circumstances.

5 During the Relevant Period, Medibank's cybersecurity and information security framework comprised the policies, standards, and resources identified in **Annexure A**.

6 Having regard to its size, resources, the nature and volume of the personal information it held (which included sensitive information, such as information about its customers' race and ethnicity and health information), and the risk of harm for an individual in the case of a breach, during the Relevant Period it was reasonable for Medibank to adopt all, or alternatively some combination sufficient to its circumstances, of the measures identified in **Annexure B** to protect the personal information it held. These measures were not implemented, or, alternatively, not properly implemented or enforced, by Medibank during the Relevant Period.

7 From at least the commencement of the Relevant Period, Medibank was aware of serious deficiencies in its cybersecurity and information security framework, including by reason of the reports and documents identified in **Annexure C**.

Medibank Data Breach

8 Prior to 7 August 2022, an employee of a Medibank contractor (**IT Service Desk Operator**) had saved his Medibank username and password for a number of Medibank accounts (**Medibank Credentials**) to his personal internet browser profile on the work computer he used to provide IT services to Medibank. When the IT Service Desk Operator subsequently signed into his internet browser profile on his personal computer, the Medibank Credentials were synced across to his personal computer.

9 The IT Service Desk Operator was a full-time employee of Medibank's third-party IT contractor, [redacted]. He was contracted by [redacted] to Medibank as an [redacted] between [redacted] and [redacted]. During the period of his employment, he had access to Medibank accounts using his Medibank Credentials including:

9.1 a standard access [redacted] account; and

9.2 an elevated access [redacted] account (**Admin Account**).

10 During the Relevant Period, the Admin Account had access to most (if not all) of Medibank's systems, including network drives, management consoles, and remote desktop access to jump box servers (used to access certain Medibank directories and databases).

11 On or around 7 August 2022, the Medibank Credentials were stolen from the IT Service Desk Operator's personal computer by a threat actor using a variant of malware known as [redacted]. Using the Medibank Credentials, a threat actor was able to:

(a) on 12 August 2022, log onto Medibank's Microsoft Exchange server and test the Medibank Credentials for the Admin Account;

(b) on or around 23 August 2022, authenticate and log onto Medibank's "Global Protect" Virtual Private Network (**VPN**) solution (which controlled remote access to the Medibank corporate network) for the first time;

(c) on or around 23 August 2022, [redacted] being a type of malicious script commonly used by threat actors; and

(d) on or around 25 August 2022, authenticate and log onto Medibank's Global Protect VPN and obtain or copy a [redacted]

[redacted]

12 The threat actor was able to authenticate and log onto Medibank's Global Protect VPN using only the Medibank Credentials because, during the Relevant Period, access to Medibank's Global Protect VPN did not require two or more proofs of identity or multi-factor authentication (**MFA**). Rather, Medibank's Global Protect VPN was configured so that only a device certificate, or a username and password (such as the Medibank Credentials), was required.

13 On or around 24 and 25 August 2022, Medibank's Endpoint Detection and Response (**EDR**) Security Software [redacted] generated various alerts in relation to the threat actor's activity that were sent to a Medibank IT Security Operations email address. These alerts were not appropriately triaged or escalated by either Medibank or its service provider, [redacted], at that time.

14 During the period from around 25 August 2022 until around 13 October 2022:

(a) using the Medibank Credentials and/or the credentials extracted from the [redacted] the threat actor accessed numerous Medibank IT systems, including:

(i) the "MPLFiler" and "Confluence" systems (the Confluence system contained information relating to how the MARS Database referred to below was structured);

(ii) [redacted] and

(iii) the MARS Database, which contained personal information of Medibank's customers, including sensitive and health information;

(b) the threat actor exfiltrated approximately 520 gigabytes of data from Medibank's systems (including the MARS Database and MPLFiler systems). This included names, dates of birth, addresses, phone numbers, email addresses, Medicare numbers, passport numbers, health related information and claims data (such as patient names, provider names, primary/secondary diagnosis and procedure codes, treatment dates). That information was personal information and sensitive information, as defined in s 6 of the Act; and

(c) [redacted] generated various further alerts in relation to the threat actor's activity, which were not appropriately triaged or escalated by either Medibank or [redacted] at the time the alerts were generated.

15 On 11 October 2022, Medibank's Security Operations team triaged a high severity incident for a [redacted] alert that identified modification of files needed to exploit the "ProxyNotShell" vulnerability. On the same day, Medibank engaged Threat Intelligence, its existing digital forensics and incident response partner, to perform an incident response investigation.

16 Until at least 16 October 2022, when a Threat Intelligence analyst noted that there had been a series of suspicious volumes of data exfiltrated out of Medibank's network, Medibank was not aware that customer data had been accessed by a threat actor and exfiltrated from its systems.

17 On 19 and 22 October 2022 respectively, Medibank was contacted by a threat actor and provided with files containing sample data that had been exfiltrated from Medibank's systems.

18 Between 9 November 2022 and 1 December 2022, a threat actor published data exfiltrated during the data breach on the dark web. The information published on the dark web included

personal information and sensitive information within the meaning of s 6 of the Act, including names, dates of birth, gender, Medicare numbers, residential addresses, email addresses, phone numbers, visa details for international worker and visitor customers, and health claims data (such as patient names, provider names, provider location and contact details, diagnosis numbers and procedure numbers and dates of treatment).

C ALLEGED CONTRAVENTIONS OF THE ACT

Breach of APP 11.1

19 During the Relevant Period, having regard to its size, resources, the nature and volume of the personal information it held (which included sensitive information, such as information about its customers' race and ethnicity and health information), and the risk of harm for an individual in the case of a breach, APP 11.1 required Medibank to take all, or alternatively some combination sufficient to its circumstances, of the steps identified in **Annexure B**, to protect the personal information it held. Medibank failed to take these steps during the Relevant Period, including by reason of the deficiencies outlined in **Annexure D**.

20 Further, or alternatively to [19] herein, during the Relevant Period, having regard to its size, resources, the nature and volume of the personal information it held (which included sensitive information, such as information about its customers' race and ethnicity and health information), and the risk of harm for an individual in the case of a breach, Medibank did not take such steps as were reasonable in the circumstances to protect the information it held from misuse, unauthorised access and/or disclosure. There were deficiencies in the form and implementation of Medibank's cybersecurity and information security framework identified in **Annexure A**, including by reason of the deficiencies outlined in **Annexure D**.

21 By reason of the matters alleged at [19] to [20] herein, during the Relevant Period, Medibank breached APP 11.1.

Contravention of s 13G of the Act

22 Under s 13(1) of the Act, an act or practice of an APP entity is an interference with the privacy of an individual if it breaches an APP in relation to the personal information about the individual.

23 By reason of the matters alleged at [19] to [22] herein, during the Relevant Period, Medibank interfered with the privacy of each of the approximately 9.7 million individuals whose personal information it held during that time.

24 Under s 13G of the Act, an entity will be liable for a civil penalty if it does an act, or engages in a practice, that is a serious or repeated interference with the privacy of an individual.

25 With respect to Medibank's interferences with the privacy of an individual (being its acts or practices in breach of APP 11.1):

(a) those acts or practices comprised serious interferences with the privacy of an individual in contravention of s 13G(a), including because of:

(i) the nature of the deficiencies in Medibank's cybersecurity and information security framework, including Medibank's failure to implement or properly configure information security controls of a basic or baseline nature or standard for an organisation of Medibank's size and in light of the volume and sensitivity of the personal information it held;

(ii) the nature of the personal information involved in the contravention, which included sensitive information such as health information and information about the individual's race and ethnicity; and