NOTICE OF FILING

Details of Filing

Document Lodged:	Concise Statement
Court of Filing	FEDERAL COURT OF AUSTRALIA (FCA)
Date of Lodgment:	19/06/2024 4:10:15 PM AEST
Date Accepted for Filing:	19/06/2024 4:10:24 PM AEST
File Number:	VID497/2024
File Title:	AUSTRALIAN INFORMATION COMMISSIONER v MEDIBANK PRIVATE LIMITED ACN 080 890 259
Registry:	VICTORIA REGISTRY - FEDERAL COURT OF AUSTRALIA

Registrar

Important Information

This Notice has been inserted as the first page of the document which has been accepted for electronic filing. It is now taken to be part of that document for the purposes of the proceeding in the Court and contains important information for all parties to that proceeding. It must be included in the document served on each of those parties.

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

Form NCF1

Concise Statement

No. 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

(iii) the consequences of the contravention, including the exposure of the individual to harm including potential emotional distress and the material risk of identity theft, extortion, and financial crime;

(b) further or alternatively, these were acts or practices that were repeatedly engaged in by Medibank in contravention of s 13G(b).

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

(a) separate contraventions of s 13G(a) arise in respect of each of the approximately 9.7 million individuals whose personal information Medibank held throughout the Relevant Period;

(b) alternatively to [26(a)] herein, a contravention of s 13G(a) arises in respect of the approximately 9.7 million individuals whose personal information Medibank held throughout the Relevant Period;

(c) further or alternatively to [26(a)-(b)] herein, a contravention of s 13G(b) arises in respect of each of the approximately 9.7 million individuals whose personal information Medibank held throughout the Relevant Period, which contravention was repeated for every day that Medibank's interferences with the privacy of those individuals subsisted during the Relevant Period.

27 Each contravention within the Relevant Period attracts a maximum penalty of $2,220,000 by reason of s 13G of the Act in force during the Relevant Period, and s 82(5)(a) of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth)).

D RELIEF SOUGHT

28 The AIC seeks the relief set out in the accompanying Originating Application, including declaratory relief under s 21 of the *Federal Court of Australia Act 1976* (Cth), orders for civil pecuniary penalties under s 80U of the Act, and costs.

E ALLEGED HARM

29 A fundamental principle underpinning the Act is that APP entities are responsible for the personal information they hold. Medibank did not have regard to this principle throughout the Relevant Period, in that it failed adequately to manage cybersecurity and/or information security risk congruent with the nature and volume of personal information it held (which included sensitive information, such as information about its customers' race and ethnicity and health information), its size, and the risk profile of organisations operating within its sector. Medibank did not invest sufficiently in the specialist cybersecurity and/or information security resources or the policies, practices and controls reasonably required to protect the personal information it held.

30 Medibank's failure to take reasonable steps commensurate with protecting the personal and sensitive information it held, exposed that information to the risk of misuse, unauthorised access and/or disclosure. That risk materialised when Medibank was the subject of a cyberattack and one or more threat actors accessed personal identifying information and health information and posted this information on the dark web, exposing approximately 9.7 million individuals to the risk of harm, including potential emotional distress and the material risk of identity theft, extortion and financial crime.

This concise statement was prepared by DLA Piper Australia, and settled by Ruth Higgins SC, Greg O'Mahoney and Amy Reid of Counsel.

Annexure A – Medibank's cybersecurity and information security framework

Policy framework

Medibank had, at least, the following cybersecurity or cybersecurity-related policies and standards in place from the dates specified:

1 Enterprise Security Policy (version 6.3), effective from November 2017.

2 Information Security Policy (version 7.0) (sets out Medibank's Information Security Documentation Framework), effective from 1 May 2021.

3 Information Security Policy (version 7.1) (sets out Medibank's Information Security Documentation Framework), effective from 26 May 2022.

4 Enterprise IT Security Principles, effective from November 2017.

5 Enterprise Security - Vulnerability Management Standard (version 1.6), dated November 2017.

6 Enterprise Security - Vulnerability Management Standard (version 1.7), effective from 1 September 2021.

7 Enterprise Security - Vulnerability Management Standard (version 2.0), effective from 1 January 2022.

8 Enterprise Security Access Control Standard (version 2.10), approved in April 2020.

9 Enterprise Security Anti-Malware Standard, approved in May 2019.

10 Enterprise Security Audit Logging Standard, approved in May 2020.

11 Enterprise Security Standard - Backup and Recovery (version 1.6), approved in November 2017.

12 Enterprise Security Standard - Cryptographic Controls (version 1.6), approved in November 2017.

13 Enterprise Security Standard - Network Design (version 1.7), approved in November 2017.

14 Enterprise Security Standard - System & Software Development (version 1.6), approved in November 2017.

15 Bring Your Own Mobile Device Policy (version 2.3), effective from December 2017.

16 Information Security BYOD Policy (version 1.0), effective from 13 September 2022.

17 Information Security Password Standard (version 1.0), effective from September 2021.

18 Enterprise Security Suppliers & Partners Standard (version 1.7), approved in September 2019.

19 Information Security Supplier Management Standard (version 2.0), approved in March 2022 and effective from April 2022.

20 IT&T Acceptable Use Policy (version 5.0), effective from May 2020.

21 IT&T Acceptable Use Policy (version 6.1), effective from 1 August 2021.

22 Medibank Zero Trust Strategy (version 1.0) dated 13 December 2021.

23 MPL Information Security Temporary Exemption Procedure (version 1.0) dated May 2020.

24 Notifiable Data Breach Reporting Policy dated 7 June 2022.

25 Third-Party Information Security Risk Management Framework (version 1.01), effective from 10 June 2021.

26 Third-Party Information Security Risk Management Procedure (version 1.01), effective from 10 June 2021.

27 Third-Party Information Security Risk Management Roles and Responsibilities (version 1.1) dated 30 March 2021.

28 User Access Audit Policy and embedded IM User Access Audit Runsheet dated 2 December 2020.

29 Crisis Management Quick Reference Guide dated 20 September 2022.

30 IT Security Incident Response Plan and Playbooks (version 1.0), approved 19 September 2022.

31 Operational Risk and Compliance Incident Management Procedure (version 3.1), approved 14 October 2020.

In addition, during the Relevant Period, Medibank had the following policy and standard documents which were not specific to cybersecurity risks from the dates specified below:

32 IT Service Management – Change Management Process (version 1.8) dated 27 January 2021.

33 IT Service Management – Change Management Process (version 1.9) dated 21 January 2022.

34 IT Service Management – Change Management Process (version 1.10) dated 28 September 2022.

35 IT Service Management – Configuration Management Process (version 1.3), covering the period of May 2020 to April 2021.

36 IT Service Management – Configuration Management Process (version 1.4) dated 9 April 2021.

37 IT Service Management – Configuration Management Process (version 1.5) dated 7 June 2021.

38 IT Service Management – Incident Management Process (version 1.6) dated 24 January 2022.

39 IT Service Management – Problem Management Process (version 1.5) dated 21 December 2021.

40 IT Service Management – Request Management Process (version 1.2) dated 12 July 2017.

41 IT Service Management – Service Catalogue Management Process dated 15 August 2017.

42 Procurement Policy, effective from 10 January 2022.

43 Procurement Policy, effective from 20 April 2022.

44 Risk Management Procedure, effective from 30 August 2020.

45 Risk Appetite Statement Policy (version 4), effective from 1 April 2022.

Resources

During the Relevant Period:

46 Medibank's core IT security function comprised a team of 13 full-time IT security professionals.

47 Medibank's FY22 information technology budget was approximately $4-5 million, of which $1 million was allocated for cyber security.

Annexure B – Steps to protect personal information held by Medibank

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 following measures to protect the personal information it held:

1 Implement MFA for authenticating remote access users to its Global Protect VPN.

2 Implement MFA for authenticating users to sensitive or critical information assets once inside its network perimeter, including important data repositories and/or servers used to connect to any such repositories.

3 Implement proper change management controls for changes made to information security controls including changes to the configuration of existing controls.

4 Implement appropriate privileged access management controls by:

(a) restricting access to and privileges in respect of information assets in accordance with the role and responsibilities of users and to the least privileges necessary; and

(b) regularly reviewing the number of privileged accounts and privileges or permissions granting to those accounts to ensure that accounts were not part of security groups that enabled greater privileged access than was required and to identify and revoke access for any dormant accounts or users.

5 Implement appropriate monitoring for privileged accounts, including by:

(a) undertaking monitoring to understand normal behaviour for privileged accounts accessing its IT systems; and

(b) configuring alerts, and monitoring any such alerts, for unusual or suspicious privileged account activities.

6 Implement appropriate password complexity for user accounts, including by implementing appropriate controls to prevent the use of insecure or common passwords and the re-use of passwords across multiple accounts.

7 Implement password monitoring and review processes to ensure that passwords used to access important data repositories and/or servers were encrypted and not stored in plain text, including by:

(a) undertaking regular password usage audits; and

(b) undertaking security assessments of tools used to access or query important data repositories and/or servers to identify whether such tools allow for passwords to be stored in plain text.

8 Implement appropriate security monitoring processes and procedures to detect and respond to information security incidents in a timely manner, including by:

(a) undertaking a first-level review and triage of all security alerts generated by Medibank's EDR Security Software;

(b) having clearly documented guidance and procedures for escalating security alerts that were not marked as benign or false positives by the first-level review team to the Medibank IT Security Operations team for further investigation;

(c) regularly reviewing the work performed by the first-level review team to ensure that security alerts were properly reviewed, triaged and escalated (where required) to reduce the likelihood of false positives and false negatives; and

(d) configuring volumetric alerts to be generated for the exfiltration of large or abnormal volumes of data from servers used to connect to sensitive or critical information assets.

9 Implement appropriate security assurance testing for sensitive or critical information assets and/or key information security controls, including by:

(a) implementing annual penetration testing for the Global Protect VPN solution and ensuring that the scope of such testing included testing of whether MFA was properly configured for authenticating remote access users to the Global Protect VPN;

(b) conducting annual internal audits and/or internal control effectiveness testing of key information security controls, including the configuration of MFA for authenticating remote access users to the Global Protect VPN and for authenticating users to other sensitive or critical information assets or servers used to access such assets, to determine if the controls have been implemented correctly and are operating as intended; and

(c) in the event that a change was made to the configuration of the Global Protect VPN which had the potential to impact the configuration of MFA for the solution, conducting internal and/or external testing to determine whether MFA was enforced for authenticating remote access users to the Global Protect VPN following the change.

10 Implement appropriate application controls for critical servers, including servers used to access sensitive or critical information assets.

11 Implement effective contractor assurance, including by:

(a) conducting regular audits, inspections and/or testing to ensure that third-party contractors with access to Medibank's IT network and IT systems were complying with Medibank's information security policies and controls identified in **Annexure A**; and

(b) where responsibility for implementing, or assisting with the implementation of, one or more information security controls was outsourced to a third-party, ensuring that the terms of the agreement and that the roles and responsibilities of the parties are clearly identified.

The reasonableness of the measures referred to above is also informed by various cybersecurity and information security standards and frameworks which existed during the Relevant Period, including the following:

1 The Australian Cyber Security Centre (**ACSC**):

(a) identified eight key controls as the controls that it considered "essential" to preventing cyberattacks (**E8**); and

(b) published the E8 Maturity Model which outlined guidance for implementing the E8 strategies.

Medibank conducted internal audits of its cybersecurity framework against the E8 controls and the E8 Maturity Model during the Relevant Period.

2 Australian Prudential Regulation Authority (**APRA**) had published Prudential Standard CPS 234 (**CPS 234**), which required Medibank, as an APRA regulated entity, to:

(a) have information security controls in place to protect its information assets against information security vulnerabilities and threats;

(b) test the effectiveness of its information security controls through a systematic testing program; and

(c) to have robust mechanisms in place to detect and respond to information security incidents.

Medibank conducted internal audits of its cybersecurity framework against CPS 234 during the Relevant Period.

3 APRA had also published Prudential Practice Guide CPG 234 Information Security with respect to the implementation of CPS 234 (**CPG 234**).

4 The Australian Signals Directorate (**ASD**) had published the Information Security Manual (**ISM**) which outlined a cyber security framework that an organisation could apply, using their risk management framework, to protect their systems and data from cyber threats.

5 The United States National Institute of Standards and Technology Cybersecurity Framework (**NIST Cyber Security Framework**). Medibank had selected the NIST Cyber Security Framework for the purposes of benchmarking its cybersecurity capabilities during the Relevant Period.

6 The International Organisation for Standardisation and International Electrotechnical Commission had published the ISO 27000 series (**ISO 27000**) of information security standards which outlined best practices for managing information security risks through the implementation of information security controls.

Annexure C – Medibank's awareness of serious deficiencies in its cybersecurity and information security framework

1 A report of a penetration test of Medibank's OSHC web environment by Threat Intelligence dated 26 March 2018 identified weaknesses in Medibank's cybersecurity framework, including insecure or weak password requirements for accessing its systems. Further penetration test reports provided by Threat Intelligence in September 2018 and November 2020 in relation to different environments identified similar deficiencies regarding insecure or weak password requirements.

2 An internal audit report provided by KPMG in or around May 2020 in relation to Medibank's compliance with APRA CPS 234 assessed Medibank's overall maturity control rating against CPS 234 as 'Developing' and identified a key focus area should be enhancing its processes for assessing the information security capabilities of third parties managing Medibank information assets.

3 An Active Directory Risk Assessment report provided by Datacom on or around 27 June 2020 identified that Medibank had an excessive number of individuals who had access to Active Directory (being the Microsoft directory service used for management of all Medibank users, group policies and domains), a number of individuals had been given excessive privileges to perform simple daily routines, and that MFA had not been enabled for privileged and non-privileged users which was described as a "critical" defect.

4 An information security internal audit report provided by KPMG in or around August 2021, which assessed the design and effectiveness of a selection of Medibank's key information security controls supporting 4 of the E8 strategies, including MFA, and the implementation of controls against E8 strategies for key IT assets, identified that MFA had not been implemented for privileged users when accessing particular systems, backend portals, or supporting servers.

5 An internal Medibank presentation prepared in around February 2022 in relation to work being undertaken to identify gaps in Medibank's compliance with CPS 234, identified that a set of security controls and a control review process and timeline for conducting the review had been prepared in 2020, but never implemented.

6 In or around July 2022, an internal audit report prepared by KPMG, or alternatively by Medibank, assessing the design and operating effectiveness of a sample of the 32 E8 Maturity Level 3 controls across the E8 mitigation strategies assessed Medibank's controls that were in scope for the audit as aligned to either Maturity Level Zero, Level 1 or Level 2. The internal audit report identified that vulnerability scanning of workstations was only being done on a representative sample of workstations, that security event monitoring should be uplifted to include unsuccessful MFA attempts, and that application control software was not in place for all servers and workstations.

7 On or around 31 August 2022, a report prepared by PricewaterhouseCoopers in relation to an independent limited assurance assessment of the design, description, and operative effectiveness of Medibank's information security controls in the period 1 June 2021 to 31 May 2022 identified deficiencies in relation to, *inter alia*, the testing of third-party information security controls.

Annexure D – Medibank's failure to take reasonable steps pursuant to APP 11.1 to protect personal information

During the Relevant Period:

1 [redacted]

2 [redacted]

3 [redacted]

4 [redacted]

5 [redacted]

6 [redacted]

7 [redacted]

8 [redacted]

9 [redacted]

10 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11 [redacted]

12 [redacted]

13 [redacted]

[redacted]

[redacted]

14 [redacted]

15 [redacted]

Certificate of lawyer

I, Gowri Kangeson, certify to the Court that, in relation to the Concise Statement 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: 5 June 2024

Signed by Gowri Kangeson
DLA Piper Australia
Lawyer for the Applicant