**IN THE SUPREME COURT OF VICTORIA**
**AT MELBOURNE**
**COMMERCIAL COURT**
**GROUP PROCEEDINGS LIST**



No. S ECI 2023 01227

BETWEEN

**ROBERT LAIRD KILAH**

First plaintiff

**BRENDAN FRANCIS SINNAMON**

Second plaintiff

AND

**MEDIBANK PRIVATE LIMITED (ACN 080 890 259)**

Defendant

# CONSOLIDATED WRIT

(Filed pursuant to the Order of Justice Attiwill made on 6 September 2023)

---

**Date of Document**: 3 October 2023

**Filed on behalf of**: Robert Kilah (First Plaintiff) and Brendan Sinnamon (Second Plaintiff)

**Prepared by:** Joint Lawyers for the Plaintiffs
Quinn Emanuel Lawyers
Level 15, 111 Elizabeth St Sydney NSW 2000
Email:
damianscattini@quinnemanuel.com

Solicitors Code: 24875
Tel: (02) 9146 3500
Ref: 11814-00001

**Phi Finney McDonald**
Level 3, 325 Flinders Lane, Melbourne VIC 3000
Email: Tania.Noonan@phifinneymcdonald.com

Solicitors Code: 110756
Tel:(03) 9134 7100
Ref: 200104

**Joint address for service:** medibankclassaction@phifinneymcdonald.com

---

TO THE DEFENDANT

TAKE NOTICE that this proceeding has been brought against you by the plaintiffs for the claim set out in this writ.

IF YOU INTEND TO DEFEND the proceeding, or if you have a claim against the plaintiffs which you wish to have taken into account at the trial, YOU MUST GIVE NOTICE of your intention by filing an appearance within the proper time for appearance stated below.

YOU OR YOUR SOLICITOR may file the appearance. An appearance is filed by—

(a) filing a "Notice of Appearance" in the Prothonotary's office, 436 Lonsdale Street, Melbourne, or, where the writ has been filed in the office of a Deputy Prothonotary, in the office of that Deputy Prothonotary; and

(b) on the day you file the Notice, serving a copy, sealed by the Court, at the plaintiff's address for service, which is set out at the end of this writ.

IF YOU FAIL to file an appearance within the proper time, the plaintiffs may OBTAIN JUDGMENT AGAINST YOU on the claim without further notice.

THE PROPER TIME TO FILE AN APPEARANCE is as follows—

(a) where you are served with the writ in Victoria, within 10 days after service;

(b) where you are served with the writ out of Victoria and in another part of Australia, within 21 days after service;

(c) where you are served with the writ in Papua New Guinea, within 28 days after service;

(d) where you are served with the writ in New Zealand under Part 2 of the *Trans-Tasman Proceedings Act 2010* of the Commonwealth, within 30 working days (within the meaning of that Act) after service or, if a shorter or longer period has been fixed by the Court under section 13(1)(b) of that Act, the period so fixed;

(e) in any other case, within 42 days after service of the writ.

**FILED 3 October 2023**

Prothonotary

**STATEMENT OF CLAIM**

## Table of Contents

## A. INTRODUCTION

### A1. The plaintiffs and Group Members

1. The plaintiffs bring this proceeding as a group proceeding against the defendant (**Medibank**) pursuant to Part 4A of the ***Supreme Court Act** 1986* (Vic) on their own behalf and on behalf of all persons (**Group Members**) who or which:

   (a) during the period 1 July 2019 to 25 October 2022 (inclusive) (**Relevant Period**):

      (i) acquired an interest in, or entered into a contract to acquire an interest in, ordinary shares in Medibank (**MPL Shares**); and/or

(ii) acquired long exposure to MPL Shares by entering into equity swap confirmations in respect of MPL Shares (**MPL Equity Swaps**);

(b) have suffered loss or damage by, because of or resulting from the conduct of Medibank pleaded in this Statement of Claim;

(c) were not during the Relevant Period, and are not as at the date of this Statement of Claim, any of the following:

(i) any of the persons referred to in s 33E(2) of the *Supreme Court Act*;

(ii) a related party (as defined by s 228 of the ***Corporations Act** 2001* (Cth)) of Medibank;

(iii) a related body corporate (as defined in s 50 of the *Corporations Act*) of Medibank;

(iv) an associated entity (as defined in s 50AAA of the *Corporations Act*) of Medibank;

(v) an officer or close associate (as defined in s 9 of the *Corporations Act*) of Medibank;

(vi) an officer or employee of, or other legal practitioner engaged by, the solicitors for the plaintiffs in relation to this proceeding.

2. The first plaintiff:

(a) acquired an interest in MPL Shares during the Relevant Period;

(b) did not dispose of any MPL Shares during the Relevant Period.

**Particulars**

The details of the acquisitions of MPL Shares by the first plaintiff are:

| ***Date*** | ***Transaction type*** | ***Number of MPL Shares*** | ***Unit Price*** |
|---|---|---|---|
| 9 July 2021 | Buy | 2,686 | $3.22 |

3. The second plaintiff:

(a) acquired an interest in MPL Shares during the Relevant Period; and

(b) did not dispose of any MPL Shares during the Relevant Period.

**Particulars**

The details of the acquisitions of MPL Shares by the second plaintiff are:

| ***Date*** | ***Transaction type*** | ***Number of MPL Shares*** | ***Unit Price*** |
|---|---|---|---|
| 26 October 2021 | Buy | 900 | $3.47 |
| 17 November 2021 | Buy | 700 | $3.50 |

4. As of the date of the commencement of this proceeding, there are seven or more persons who have claims against Medibank in respect of the matters set out herein.

**A2. Medibank**

5. Medibank:

(a) is and was at all material times a company registered under the *Corporations Act* and capable of being sued;

(b) is and was at all material times a person within the meaning of s 1041H of the *Corporations Act*;

(c) is and was at all material times a person within the meaning of s 12DA of the *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**);

(d) is was at all material times a person within the meaning of s 18 of the Australian Consumer Law set out in Schedule 2 to the *Competition and Consumer Act 2010* (Cth), as applied by the following statutes (individually or collectively, the **ACL**):

(i) s 7 of the *Fair Trading Act (Australian Consumer Law) Act 1992* (ACT);

(ii) s 28 of the *Fair Trading Act 1987* (NSW);

(iii) s 8 of the *Australian Consumer Law and Fair Trading Act 2012* (Vic);

(iv) s 16 of the *Fair Trading Act 1989* (Qld);

(v) s 6 of the *Australian Consumer Law (Tasmania) Act 2010* (Tas);

(vi) s 19 of the *Fair Trading Act 2010* (WA);

(vii) s 14 of the *Fair Trading Act 1987* (SA); and/or

(viii) s 27 of the *Consumer Affairs and Fair Trading Act 1990* (NT);

(e) is and was at all material times a "listed disclosing entity" within the meaning of s 674 of the *Corporations Act*; and

(f) has since 14 August 2021 been a "listed disclosing entity" within the meaning of s 674A of the *Corporations Act*.

6. At all times in the Relevant Period, Medibank was the parent entity of a consolidated group of companies that included Australian Health Management Group Pty Ltd (ACN 004 683 298) (**ahm**) as a wholly owned subsidiary.

**A3. Directors and other officers of Medibank**

7. Elizabeth Alexander AO was:

(a) from March 2013 to 1 October 2020, Chairman of the Board of Medibank;

(b) from March 2014 to 30 June 2017, a member of the Audit and Risk Management Committee;

(c) from 1 July 2017 to 1 October 2020, a member of Medibank's Audit Committee (**Audit Committee**);

(d) from 1 July 2017 to 1 October 2020, a member of Medibank's Risk Management Committee (**Risk Management Committee**); and

(e) at all times from the start of the Relevant Period to 1 October 2020, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

**Particulars**

The plaintiffs refer to listing rule 19.3(a) of the ASX Listing Rules as in force during the Relevant Period, which provided that expressions that are not specifically defined in the ASX Listing Rules but are given a particular meaning in the *Corporations Act*, have the same meaning in the ASX Listing Rules.

8. Mike Wilkins AO was:

(a) from 1 October 2020 to the end of the Relevant Period, Chairman of the Board of Medibank;

(b) from 1 October 2020 until 21 May 2021 and later from 18 November 2021 to 31 March 2022, a member of the Audit Committee;

(c) from 1 July 2017 to 21 May 2021, a member of Risk Management Committee; and

(d) at all times from 1 October 2020 to the end of the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

9. Craig Drummond was:

(a) from 4 July 2016 until 17 May 2021, Chief Executive Officer of Medibank; and

(b) at all times from the start of the Relevant Period until 17 May 2021, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

10. David Koczkar (**Koczkar**) was:

(a) from 31 March 2014 to September 2016, Chief Operating Officer of Medibank;

(b) from about April 2016 to June 2016, Acting Chief Executive Officer of Medibank;

(c) from September 2016 to 17 May 2021, Chief Customer Officer of Medibank;

(d) from 17 May 2021 to the end of the Relevant Period, Chief Executive Officer of Medibank; and

(e) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

11. Tracey Batten was:

(a) from 28 August 2017 to the end of the Relevant Period, a non-executive member of the Board of Medibank;

(b) from 28 August 2017 to the end of the Relevant Period, a member of the Risk Management Committee; and

(c) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

12. Anna Bligh AC was:

(a) from December 2012 to the end of the Relevant Period, a non-executive member of the Board of Medibank;

(b) from 31 March 2022 to the end of the Relevant Period, a member of the Risk Management Committee; and

(c) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

13. Gerald Dalbosco was:

(a) from 21 May 2021 to the end of the Relevant Period, a non-executive member of the Board of Medibank;

(b) from 21 May 2021 to 18 November 2021, a member of the Audit Committee;

(c) from 18 November 2021 to the end of the Relevant Period, Chairman of the Audit Committee;

(d) from 21 May 2021 to the end of the Relevant Period, a member of the Risk Management Committee; and

(e) at all times from 21 May 2021 to the end of the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and Listing Rule 19.12.

14. Peter Everingham was:

(a) from 31 March 2022 to the end of the Relevant Period, a non-executive member of the Board of Medibank;

(b) from 31 March 2022 to the end of the Relevant Period, a member of the Audit Committee; and

(c) at all times from 31 March 2022 to the end of the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

15. Kathryn Fagg AO was:

(a) from 31 March 2022 to the end of the Relevant Period, a non-executive member of the Board of Medibank;

(b) from 31 March 2022 to the end of the Relevant Period, a member of the Audit Committee; and

(c) at all times from 31 March 2022 to the end of the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

16. Linda Bardo Nicholls AO was:

(a) from 31 March 2014 to the end of the Relevant Period, a non-executive member of the Board of Medibank;

(b) from 1 June 2022 to the end of the Relevant Period, a member of the Audit Committee; and

(c) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

17. Peter Hodgett was:

(a) from June 2013 to 18 November 2021, a non-executive member of the Board of Medibank;

(b) from 1 July 2017 to 18 November 2021, a member of the Audit Committee; and

(c) at all times from the start of the Relevant Period to 18 November 2021, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

18. Christine O'Reilly was:

(a) from 31 March 2014 until 18 November 2021, a non-executive member of the Board of Medibank;

(b) from 1 July 2017 until 18 November 2021, Chairman of the Audit Committee;

(c) from 1 July 2017 until 18 November 2021, a member of the Risk Management Committee; and

(d) at all times in the Relevant Period until 18 November 2021, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

19. David Fagan was:

(a) from 31 March 2014 to the end of the Relevant Period a non-executive member of the Board of Medibank;

(b) from 18 November 2021 to the end of the Relevant Period, a member of the Audit Committee;

(c) from 1 July 2017 to the end of the Relevant Period, Chairman of Risk Management Committee; and

(d) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

20. Mark Rogers was:

(a) from 3 January 2017 to May 2021, Chief Financial Officer of Medibank;

(b) from May 2021 to the end of the Relevant Period, Group Executive – Chief Financial Officer & Group Strategy at Medibank; and

(c) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

21. Mei Ramsay was:

(a) from 14 September 2016 to the end of the Relevant Period, Group Executive – Legal, Governance & Compliance at Medibank;

(b) from October 2014 to the end of the Relevant Period, Company Secretary of Medibank; and

(c) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

22. Rob Deeming was:

(a) from about June 2021 to present, Group Executive – Customer & Brands at Medibank; and

(b) at all times from about June 2021 to the end of the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

23. John Goodall was:

(a) from December 2016 to the end of the Relevant Period, Executive General Manager – Technology & Operations at Medibank; and

(b) at all times in the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

24. Milosh Milisavljevic was:

(a) from 22 June 2021 to the end of the Relevant Period, Group Executive – Customer Portfolios at Medibank; and

(b) at all times from 22 June 2021 to the end of the Relevant Period, an officer of Medibank within the meaning of s 9 of the *Corporations Act* and the ASX Listing Rules.

## B. MEDIBANK'S BUSINESS AND THE CONTEXT IN WHICH IT OPERATED

### B1. Medibank's business

25. At all times in the Relevant Period, Medibank:

(a) was Australia's largest private health insurer;

(b) was a "private health insurer" within the meaning of the ***Private Health Insurance Act** 2007* (Cth);

(c) carried on a health insurance business within the meaning of the *Private Health Insurance Act*;

(d) was registered under Division 3 of Part 2 of the *Private Health Insurance (Prudential Supervision) Act 2015* (Cth) (**Private Health Supervision Act**) and, in the premises, was a "private health insurer" within the meaning of the Private Health Supervision Act; and

(e) was a provider of private health insurance to holders of private health insurance policies (as that term was defined in the *Private Health Insurance Act*):

(i) under the "Medibank" brand (**Medibank Customers**); and

(ii) under the "ahm" or "ahm health insurance" brand (**ahm Customers**).

26. At all times in the Relevant Period, during the course of, or for the purpose of, its business, Medibank collected, stored and accessed electronically information relating to Medibank Customers and ahm Customers and their claims made under health insurance policies (including names, dates of birth, addresses, phone numbers, email addresses, passport numbers, information about where customers received certain medical services, and codes associated with diagnoses and procedures administered) (**Personal and Sensitive Data and Health Claims Information**), such information including:

(a) identification information about individuals within the meaning of the ***Privacy Act** 1988* (Cth);

(b) personal information within the meaning of the *Privacy Act*;

(c) sensitive information within the meaning of the *Privacy Act*; and

(d) health information within the meaning of the *Privacy Act*.

**Particulars**

A. At all material times, the *Privacy Act* defined "identification information" about an individual as (s 6):

(a) the individual's full name, an alias or previous name;

(b) the individual's date of birth;

(c) the individual's sex;

(d) the individual's current or last known address and two previous addresses (if any);

(e) the individual's current or last known employer; or

(f) if the individual held a driver's licence—the individual's driver's licence number.

B. At all material times, the *Privacy Act* defined "personal information" as (s 6) information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether or not the information or opinion is true or not; and

(b) whether the information or opinion is recorded in material form or not.

C. At all material times, the *Privacy Act* defined sensitive information as (s 6):

(a) information or an opinion about an individual's:

(i) racial or ethnic origin;

(ii) political opinions;

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information (as that term is defined in the *Privacy Act*) about an individual;

(c) genetic information about an individual that is not otherwise health information; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

D. At all material times, the *Privacy Act* defined "health information" as (s 6FA):

(a) information or an opinion about:

(i) the health, including an illness, disability or injury (at any time) of an individual;

(ii) an individual's expressed wishes about the future provision of health services to the individuals;

(iii) the health service provided, or to be provided to an individual;

that is also personal information;

(b) other personal information (as that term is defined in the *Privacy Act*) collected to provide, or in providing, a health service to an individual;

(c) other personal information (as that term is defined in the *Privacy Act*) collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; or

(d) genetic information about the individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

E. Document entitled "ahm by Medibank – Privacy Policy" available on ahm's website by at least 2016.

F. Document entitled "Medibank Privacy Policy" dated May 2015 (copies of which are in the possession of the solicitors for the plaintiffs and are available for inspection).

G. Medibank Privacy Policy available at https://www.medibank.com.au/privacy/ (accessed 29 June 2023).

H. Further particulars may be provided following discovery and the filing of expert evidence.

**B2. Cyber-attack risks faced by Medibank**

27. At all times in the Relevant Period, there was a risk that Medibank's systems used to collect, store and access Personal and Sensitive Data and Health Claims Information of Medibank Customers and ahm Customers would be a target of cyber-related attacks and cybercrime (**Cyber Attack Risk**), by reason of:

(a) the fact that Medibank held Personal and Sensitive Data and Health Claims Information; and

(b) the fact that, in the Relevant Period, malicious cyber actors were targeting health-sector organisations holding information such as Personal and Sensitive Data and Health Claims Information.

**Particulars**

A. Data breaches and data spills are described by the Australian Signals Directorate (**ASD**) Australian Cyber Security Centre (**ACSC**) as cyber threats: ACSC, "Threats" available at *https://www.cyber.gov.au/threats* and ACSC, "Watch out for threats", available at *https://www.cyber.gov.au/learn-basics/explore-basics/threats* (each accessed 29 June 2023).

B. In the report of the Office of the Australian Information Commissioner (**OAIC**) entitled "Notifiable Data Breaches Report: July–December 2019", dated 28 February 2020, OAIC reported as follows:

   a. "Key findings for the July to December 2019 reporting period: … The health sector is again the highest reporting sector, notifying 22 per cent of all breaches (p 3).

   b. "Top industry sectors to notify breaches … Health service providers (the health sector) reported 117 data breaches during the reporting period. This sector has consistently reported the most data breaches compared to other industry sectors since the start of the NDB scheme" (p 5). See also p 18.

C. In and from 8 May 2020, ACSC identified that "Advanced Persistent Threat" actors (also known as APT actors) are actively targeting health sector organisations and medical research facilities and that Australia's health or research sectors could be at greater threat of being targeted, and potentially compromised, by malicious APT groups: 2020-009: "Advanced Persistent Threat (**APT**) actors targeting Australian health sector organisations and COVID-19 essential services" (**2020-009 Paper**) (p 1).

D. In and from 8 May 2020, the ACSC warned that malicious actors view health sector entities as a lucrative target for ransomware attacks because of the sensitive personal and medical data they hold, and how critical this data is to maintaining operations and patient care: 2020-009 Paper (p 1).

E. In and from 8 May 2020, the ACSC warned that sophisticated actors have also been seen undertaking brute force attacks using a trial-and-error method to guess login credentials, and password spray attacks that attempt to access numerous accounts with a list of commonly-used passwords. The ACSC warned that attacks such as these often result in the theft of sensitive data, and underscore the importance of a strong cyber security culture amongst employees, including adopting multi-factor authentication, strong password policies, and regular reviews of network logs for signs of malicious activity. The exploitation of compromised Remote Desktop

Protocol credentials by malicious actors was also identified by the ACSC as a significant concern: 2020-009 Paper (p 1).

F. In and from 8 May 2020, the ACSC advised that APT actors use a range of tradecraft including combinations of high-end hacking tools and are not above using relatively simply or basic techniques such as phishing to achieve their goal. ACSC warned that APTs are patient adversaries, known to undertake detailed reconnaissance of high-value networks over months or sometimes years. The ACSC also warned that APT actors pose the most significant threat to Australia's national security and economic prosperity: 2020-009 Paper (p 2).

G. In and from 8 May 2020, the ACSC warned that a particular threat to the health sector is transactional cybercrime syndicates and their affiliates, who develop, share, sell and use sophisticated tools and techniques. The ACSC warned that there was a booming underground marketplace offering cybercrime as a service, or access to high-end hacking tools, that were once only available to nation states. The ACSC advised that the line between state sponsored actors and cybercriminals was becoming increasingly blurred and that the bar for entry was lower than ever. The ACSC stated that malicious actors with minimal technical expertise can now purchase illicit tools and services to generate alternative income streams, launder the proceeds of traditional crimes or undertake network intrusions on behalf of more sophisticated adversaries: 2020-009 Paper (pp 2-3).

H. In and from 8 May 2020, the ACSC advised health sector organisations to remain vigilant against the threat posed by APT and cybercrime actors and to ensure that their networks are protected from malicious cyber actors: 2020-009 Paper (p 3).

I. In and from 8 May 2020, the ACSC recommended that organisations in the health sector implement the ASD Essential Eight (**Essential 8**) mitigations to mitigate threats of most methodologies used by APT actors to compromise computer, specifically (2020-009 Paper at pp 3-5):

    a. enabling multi-factor authentication which is identified by the ACSC as one of the most effective controls an organisation can implement to prevent an adversary from gaining unauthorised access to a device or network and then compromising sensitive information;

    b. blocking macros from the internet, and only allowing execution of vetted and approved macros;

    c. implementing regular patching of systems and applications in a timely fashion;

    d. making regular back-ups of critical systems and databases to ensure quick and easy restoration of critical systems and services and keeping back-ups separate from corporate computers, on separate devices or using secure cloud services;

    e. alerting and educating staff;

    f. email content scanning;

g. developing and updating incident response plans;

h. implementing network segmentation and segregation as APT actors use techniques that allow them to move laterally within an organisation network. Partitioning of networks into smaller networks or developing and enforcing rulesets for controlling communications between specific hosts and services. When implementing network segmentation and segregation, restricting the level of access to sensitive information, hosts and servers. Ensure that network segmentation and segregation measures are carefully planned, robustly enforced, closely monitored and implemented in a manner that ensures that the security controls cannot be bypassed.

J. In around 8 April 2020, the United Kingdom's National Cyber Security Centre (**NCSC**) and the United States Department of Homeland Security (**DHS**) and Cybersecurity and Infrastructure Security Agency (**CISA**) issued a joint advisory regarding ongoing activity by APT groups against organisations involved in both national and international COVID-19 responses. It described APT actors as actively targeting organisations involved in both national and international COVID-19 responses, including healthcare bodies, pharmaceutical companies, academia, medical research organisations, and local government. It described password spraying as a commonly used style of brute force attack in which the attacker tries a single and commonly used password against many accounts before moving on to try a second password: NCSC, DHS and CISA, "Advisory: APT groups target healthcare and essential services", May 2020.

K. In around 2 August 2020, the ACSC issued a publication entitled "2020-013 Ransomware targeting Australian aged care and healthcare sectors" (**2020-013 Paper**). In the 2020-013 Paper, the ACSC stated that it is aware of recent ransomware campaigns targeting the aged care and healthcare sectors and that cybercriminals view the aged care and healthcare sectors as lucrative targets for ransomware attacks due to the personal and medical information held by them, and how critical that information is to maintaining operations and patient care. In the 2020-013 Paper, ASCS referred to the "Maze" ransomware and stated it was designed to lock or encrypt an organisation's valuable information and has been observed being used alongside other tools which steal important business information. ACSC stated that cybercriminals may then threaten to post this information online unless a further ransom is paid: 2020-013 available at https://www.cyber.gov.au/about-us/advisories/2020-013-ransomware-targeting-australian-aged-care-and-healthcare-sectors (accessed 29 June 2023).

L. In a publication entitled "2020 Sector Snapshot: Health" (**2020 Health Snapshot**) the ACSC warned that COVID-19 has fundamentally changed the cyber threat landscape for the health sector, with malicious actors increasingly targeting and compromising health networks (p 1). The ACSC warned that malicious actors are primarily financially motivated and may seek to gain access to valuable data stores, use the branding from high-profile victims and incidents to bolster the legitimacy of the targeting activity, and/or cause disruption to business operations and continuity through methods such as ransomware (p 1). The ACSC assessed that

ransomware is currently the most significant cybercrime threat to the Australian health sector (p 1). The ACSC stated that in the period 1 January 2020 to 31 December 2020, the ACSC had received 166 cyber security incident reports relating to the health sector, being an increase from 90 reported incidents affecting the health sector during the 2019 calendar year (p 1). The ACSC warned that the heath sector remains a valuable and vulnerable target for malicious cyber activity because of, *inter alia*, its highly sensitive personal data holdings (including information to commit identity theft or sell the data in cybercrime marketplaces), the criticality of services delivered by the health sector and the public trust in health sector organisations, particularly those linked to Government services (pp 2 and 4). The 2020 Health Snapshot stated that the targeting of the health sector by malicious actors has the potential to interfere with service delivery, impede the supply of critical products to those in need, cause reputational and financial damage to health organisation and threaten the delivery of health services and the lives of patients (p 3). The ACSC warned that common sources of compromise include hardcoded passwords, improper authentication or passwords held in recoverable areas and that remote access solutions should be reviewed to ensure industrial control systems and critical devices are effectively segmented from the remaining network (p 5). The ACSC warned that essential steps for managing remote access solutions include enabling multi-factor authentication, ensuring appropriate logging and regularly patching remote access clients and that logs should be routinely reviewed, and attention should be given to the locations and access times to ensure remote access is being utilised by legitimate staff only (p 5).

M. Further particulars may be provided following discovery and/or expert evidence.

28. At all times in the Relevant Period, if the Personal and Sensitive Data and Health Claims Information of Medibank Customers and ahm Customers was accessed, exfiltrated and/or disseminated by malicious cyber actors, or was the subject of threats to disseminate that information, this was likely to have adverse consequences for those customers (**Cyber Attack Risk Customer Consequences**), including:

(a) emotional distress;

(b) anxiety;

(c) embarrassment;

(d) humiliation;

(e) identity theft or fraud (including a heightened risk of such identity theft or fraud occurring); and/or

(f) time and expenses incurred in respect of rectification activities, including increased monitoring for fraud, obtaining new identification documents, and/or changing health insurance providers.

29. At all times in the Relevant Period, Medibank knew of the Cyber Attack Risk.

## B3. The relevant regulatory landscape with respect to the collection, storage and processing of Personal and Sensitive Data and Health Claims Information

*B3.1 The Privacy Act and the Australian Privacy Principles*

30. At all times in the Relevant Period, Medibank was:

(a) an "organisation" within the meaning of s 6C(1) of the *Privacy Act*;

(b) an "APP entity" within the meaning of s 6(1) of the *Privacy Act*; and

(c) by reason of the matters pleaded in subparagraphs (a) and (b) above, required by s 15 of the *Privacy Act* not to do an act, or engage in a practice, that breached an Australian Privacy Principle.

31. At all times in the Relevant Period, the objects of the *Privacy Act* included:

(a) to promote the protection of the privacy of individuals (s 2A(a));

(b) to provide the basis for nationally consistent regulation of privacy and the handling of personal information (s 2A(c));

(c) to promote responsible and transparent handling of personal information by entities (s 2A(d));

(d) to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)); and

(e) to implement Australia's international obligation in relation to privacy (s 2A(h)).

32. At all times in the Relevant Period, an APP entity was obliged by s 15 of the *Privacy Act* and Australian Privacy Principle 1.2 to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) would ensure that the entity complied with the Australian Privacy Principles and a registered APP code (if any) that bound the entity; and

(b) would enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

33. At all times in the Relevant Period, an APP entity holding personal information about an individual that was collected for a particular purpose was obliged by s 15 of the *Privacy Act* and Australian Privacy Principle 6.1 not to use or disclose the information for another purpose unless:

(a) the individual had consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 of Australian Privacy Principle 6 applied in relation to the use or disclosure of personal information about an individual.

34. At all times in the Relevant Period, an APP entity holding personal information was obliged by s 15 of the *Privacy Act* and Australian Privacy Principle 11.1 to take such steps as were reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

35. At all times in the Relevant Period, an APP entity holding personal information about an individual was obliged by s 15 of the *Privacy Act* and Australian Privacy Principle 11.2 to take such steps as were reasonable in the circumstances to destroy the information or to ensure that it was de-identified where the entity no longer needed the information for any purpose for which the information might be used or disclosed by the entity and:

(a) the information was not contained in a Commonwealth record; and

(b) the entity was not required by or under an Australian law, or a court/tribunal order, to retain the information,

36. Paragraphs 30 to 35 above, individually or collectively, are referred to herein as **Australian Privacy Laws**.

*B3.2 Australian Prudential Regulation Authority Prudential Standards*

37. At all material times:

(a) s 92 of the Private Health Insurance Supervision Act provided that the Australian Prudential and Regulation Authority (**APRA**) may, in writing, make standards, relating to prudential matters, that must be complied with by, or in relation to, private health insurers; and

(b) s 94 of the Private Health Insurance Supervision Act provided that a private health insurer must comply with prudential standards that apply in relation to the insurer.

38. In March 2018, APRA released for consultation a draft of Prudential Standard CPS 234 Information Security.

39. On 30 November 2018, APRA made "Banking, Insurance, Life Insurance, Health Insurance and Superannuation (prudential standard) determination No. 1 of 2018 – Prudential Standards CPS 234 Information Security" under *inter alia* s 92 of the Private Health Insurance Supervision Act (**CPS 234**).

40. CPS 234 commenced on 1 July 2019, save that, where an APRA-regulated entity's "information assets" were managed by a third party, the requirements in the standard applied in relation to those information assets from the earlier of:

(a) the next renewal date of the contract with the third party; or

(b) 1 July 2020.

**Particulars**

"Information asset" was and is defined in CPS 234 as "information and information technology, including software, hardware and data (both soft and hard copy)".

41. On 3 May 2019, APRA made "Banking, Insurance, Life Insurance and Health Insurance (prudential standard) determination No.1 of 2019 – Prudential Standard CPS 220 Risk Management" under *inter alia* section 92 of the Private Health Insurance Supervision Act (**CPS 220**).

42. CPS 220 commenced on 1 July 2019.

43. At all times in the Relevant Period, each of Medibank and ahm was:

(a) as pleaded above, a "private health insurer" within the meaning of the Private Health Insurance Supervision Act; and

(b) an "APRA-regulated entity" within the meaning of CPS 234 and CPS 220 (collectively, the **applicable Prudential Standards**).

44. At all times in the Relevant Period, each of Medibank and ahm was, by reason of the matters pleaded in paragraphs 37, 40, 42 and 43 above, obliged to comply with CPS 234 and CPS 220.

45. At all times in the Relevant Period, the Board of an APRA-regulated entity was obliged by paragraph 13 of CPS 234 to ensure that the entity maintained information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.

46. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 15 of CPS 234 to maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enabled the continued sound operation of the entity.

47. At all times in the Relevant Period, where information assets were managed by a related party or third party, an APRA-regulated entity was obliged by paragraph 16 of CPS 234 to assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.

48. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 17 of CPS 234 to actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.

49. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 18 of CPS 234 to maintain an information security policy framework commensurate with its exposures to vulnerabilities and threat.

50. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 21 of CPS 234 to must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with:

    (a) vulnerabilities and threats to the information assets;

    (b) the criticality and sensitivity of the information assets;

    (c) the stage at which the information assets are within their life-cycle; and

    (d) the potential consequences of an information security incident.

51. At all times in the Relevant Period, where an APRA-regulated entity's information assets were managed by a related party or third party, the APRA-regulated entity was obliged by paragraph 22 of CPS 234 to evaluate the design of that party's information security controls that protect the information assets of the APRA-regulated entity.

52. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 23 of CPS 234 to have robust mechanisms in place to detect and respond to information security incidents in a timely manner.

53. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 27 of CPS 234 to test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing was required to be commensurate with:

    (a) the rate at which the vulnerabilities and threats change;

    (b) the criticality and sensitivity of the information asset;

    (c) the consequences of an information security incident;

    (d) the risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies; and

    (e) the materiality and frequency of change to information assets.

54. At all times in the Relevant Period, where an APRA-regulated entity's information assets were managed by a related party or a third party, and the APRA-regulated entity was reliant on that party's information security control testing, the APRA-regulated entity was obliged by paragraph 28 of CPS 234 to assess whether the nature and frequency of testing of controls in respect of those information assets was commensurate with paragraphs 27(a) to (e) of CPS 234.

55. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 29 of CPS 234 to escalate and report to the Board or senior management any testing results that identified information security control deficiencies that could not be remediated in a timely manner.

56. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 30 of CPS 234 to ensure that testing was conducted by appropriately skilled and functionally independent specialists.

57. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 31 of CPS 234 to review the sufficiency of the testing program at least annually or when there was a material change to information assets or the business environment.

58. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 32 of CPS 234 to ensure its internal audit activities include a review of the design and operating

effectiveness of information security controls, including those maintained by related parties and third parties.

59. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 33 of CPS 234 to ensure that the information security control assurance was provided by personnel appropriately skilled in providing such assurance.

60. At all times in the Relevant Period, an APRA-regulated entity's internal audit function was required by paragraph 34 of CPS 234 to assess the information security control assurance provided by a related party or third party where:

    (a) an information security incident affecting the information assets had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and

    (b) internal audit intended to rely on the information security control assurance provided by the related party or third party.

61. At all times in the Relevant Period, the Board of an APRA-regulated entity was obliged by paragraph 9(c), (d) and (f) of CPS 220 to ensure that:

    (a) senior management of the institution monitored and managed all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the Board;

    (b) the operational structure of the institution facilitated effective risk management; and

    (c) sufficient resources were dedicated to risk management.

62. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 19 of CPS 220 to maintain a risk management framework for the institution that enabled it to appropriately develop and implement strategies, policies, procedures and controls to manage different types of material risks, and provide the Board with a comprehensive institution-wide view of material risk.

63. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 37 of CPS 220 to have a designated risk management function for the institution that, at a minimum:

    (a) was responsible for assisting the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution to maintain the risk management framework;

(b) was appropriate to the size, business mix and complexity of the institution;

(c) was operationally independent;

(d) had the necessary authority and reporting lines to the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution to conduct its risk management activities in an effective and independent manner;

(e) was resourced with staff who had clearly defined roles and responsibilities and who possessed appropriate experience and qualifications to exercise those responsibilities;

(f) had access to all aspects of the institution that had the potential to generate material risk, including information technology systems and systems development resources; and

(g) was required to notify the Board of any significant breach of, or material deviation from, the risk management framework.

64. At all times in the Relevant Period, an APRA-regulated entity was obliged by paragraph 38 of CPS 220 to designate a person to be responsible for the functions described in paragraph 37 of CPS 220, referred to as a "Chief Risk Officer".

*B3.3 Medibank's Essential Cyber Security Requirements*

65. By reason of the matters pleaded in paragraphs 25 to 64 above, at all times in the Relevant Period, Medibank was required to implement and maintain a level of information security and privacy protection and controls in respect of its information technology systems, platforms and databases (collectively, **IT Systems**) commensurate with the criticality and sensitivity of the Personal and Sensitive Data and Health Claims Information in order to protect that information from:

(a) misuse, interference and loss; and/or

(b) unauthorised access, modification, collection or disclosure.

**Particulars**

Having regard to the nature of the business conducted by Medibank as pleaded in paragraphs 5, 6 and 25 above, the criticality and sensitivity of the information held by Medibank about Medibank Customers and ahm Customers as pleaded in paragraph 26 above, the Cyber Attack Risk as pleaded in paragraph 27 above, and the Cyber Attack Risk Customer Consequences as pleaded in paragraph 28 above, the level of information security and privacy protection

required to implement and maintain an appropriate IT System and practices consistent with the standards, objects and outcomes described below, involved:

A. Remote access is managed: National Institute of Standards and Technology (**NIST**) "Framework for Improving Critical Infrastructure Cybersecurity', version 1.1 (April 2018) (**NIST Framework**) PR.AC 3; security measures implemented when personnel are working remotely to protect information accessed, processed or stored outside Medibank's premises: International Standard ISO/IEC 27001, "Information security, cybersecurity and privacy protection—Information security management systems—Requirements", (2022) (**ISO 2022**) A.6.7.

B. Network integrity is protected via network segregation and network segmentation, firewalling, segregating high-risk applications and implementing application controls to restrict or prohibit lateral movement throughout the network to locate and access sensitive information, hosts and services: NIST Framework PR.AC 5; networks managed and controlled to protect information in systems and applications: International Standard ISO/IEC 27001, "Information technology—Security techniques—Information security management systems—Requirements", (2013) (**ISO 2013**) A.13.1.1; ISO 2022 A.8.20 and the Essential 8; ACSC "Implementing Network Segmentation and Segregation" (October 2012, updated October 2021).

C. Using a number of techniques and technologies when implementing network segmentation and segregation to protect against network intrusion (such as requiring appropriate additional digital security certificates or multi-factor authentication) implemented on workstations and servers to restrict inbound and outbound network connections to an organisation's approved set of applications and services: ACSC, "Information Security Manual", (2022) (**ISM**) Control ISM-1416 and the Essential 8.

D. Configurations such as security configurations of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed: ISO 2022 A.8.9; a baseline configuration of information technology/industrial control systems is created and maintained: NIST Framework PR.IP-1.

E. Users, devices and other assets are authenticated commensurate with the risk of the transaction (for example individuals' security and privacy risks and organisational risks): NIST Framework PR.AC 7; secure authentication technologies and procedures implemented based on information access restrictions and topic-specific policy on access control: ISO 2022 A.8.5; Where required by the access control policy, access to systems and applications be controlled by a secure log-on procedure: ISO 2013 A.9.4.2.

F. Multi-factor authentication is used to authenticate unprivileged users of systems: ISM Control ISM-0974 and the Essential 8.

G. Multi-factor authentication is used to authenticate privileged users of systems: ISM Control ISM-1173 and the Essential 8.

H. Multi-factor authentication is used to authenticate users accessing important data repositories: ISM Control ISM 1505 and the Essential 8.

I. Security mechanisms, service levels and service requirements of network services identified, implemented and monitored: ISO 2022 A.8.21; security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced: ISO 2013 A.13.1.2.

J. The information system and assets are monitored to identify cybersecurity events: NIST Framework DE.CM 1.

K. External service provider activity is monitored to detect potential cyber security events: NIST Framework DE.CM 6; monitoring for unauthorised personnel, connections, devices and software: NIST DE.CM 7.

L. Networks, systems and applications monitored for anomalous behaviour: ISO 2022 A.8.16; monitoring and logging of events: ISM Controls ISM-0582, ISM-0109, ISM-1228, ISM-1537; NIST Framework PR.PT.1; anomalous activity is detected in a timely manner and the potential impact of events is understood: NIST Framework DE.AE-1, DE.AE-3, DE.AE-4 and DE.AE-5.

M. Cyber threat intelligence is received from information sharing forums and sources: NIST Framework ID.RA-2; ISO 2022 A.5.7; threats, vulnerabilities, likelihoods and impacts are used to determine risk: NIST Framework ID.RA-5.

N. Testing the effectiveness of its information security controls through a systematic testing program, the nature and frequency to be commensurate with:

a. the rate at which the vulnerabilities and threats change;

b. the criticality and sensitivity of the information asset;

c. the consequences of an information security incident;

d. the materiality and frequency of change to information assets (CPS 234, paragraph 27);

F. Review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties: CPS 234, paragraph 32.

G. Reasonable steps are taken to destroy or de-identify personal information where it is no longer needed for a permitted purpose: Australian Privacy Principle 11.2. Particulars of the reasonable steps will be provided following the filing of expert evidence.

H. Further particulars may be provided following discovery and the filing of expert evidence.

66. Further, by reason of the matters pleaded in paragraphs 25 to 64 above, Medibank was required to:

(a) implement and maintain systems, frameworks, policies or plans in respect of cyber security and resilience that were appropriate to manage the Cyber Attack Risk; and

(b) implement and maintain information security and privacy protection and controls on its IT Systems that were appropriate to the existence of the Cyber Attack Risk.

**Particulars**

A. Cyber resilience is the ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents: ACSC website at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents (accessed 29 June 2023).

B. The plaintiffs refer to and repeat the particulars subjoined to paragraph 65 above.

C. Further particulars may be provided following discovery and the filing of expert evidence.

67. Paragraphs 65 and 66 above, individually or collectively, are referred to herein as the **Essential Cyber Security Requirements**.

*B3.4 Office of the Australian Information Commissioner & the Australian Prudential Regulation Authority*

68. At all times in the Relevant Period, by reason of the matters pleaded in paragraphs 6, 26 and 30 above, Medibank and ahm's compliance with Australian Privacy Laws has been subject to regulation by the Australian Information Commissioner (**Information Commissioner**).

69. By reason of the matters pleaded in paragraph 68 above, at all times in the Relevant Period, the Information Commissioner has had the power under the *Privacy Act* to *inter alia*:

(a) conduct assessments as to whether personal information held by an APP entity, including Medibank and ahm, is being maintained and handled in accordance with the Australian Privacy Principles (s 33C(1)(a));

(b) investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made under s 36 of the *Privacy Act* (including a representative complaint where the conditions in s 38 are satisfied) (s 40(1));

(c) on the Information Commissioner's own initiative, investigate an act or practice if the act or practice may be an interference with the privacy of an individual or a breach of Australian Privacy Principles, where the Information Commissioner thinks it is desirable that the act or practice be investigated (s 40(2)); and

(d) after investigating a complaint, make a declaration that the complainant is entitled to a specified amount by way of compensation (s 52(1)(iii)).

70. At all material times in the Relevant Period, by reason of the matters pleaded in paragraphs 6, 25, 43 and 44 above, APRA has had the power under the Private Health Supervision Act:

(a) where the conditions specified in s 96 of the Private Health Supervision Act are satisfied, to give a private health insurer such as Medibank a direction of a kind specified in s 97 of the Private Health Supervision Act, including *inter alia* a direction (s 97(1)(a)(i) and (ii)):

(i) to comply with all, or all specified:

(A) enforceable obligations; or

(B) provisions of the *Financial Sector (Collection of Data) Act 2001* (Cth);

(ii) to remove an officer of the insurer from office (s 97(1)(b));

(iii) to ensure an officer of the insurer does not take part in the management or conduct of the business of the insurer except as permitted by APRA (s 97(1)(c);

(iv) to appoint a person as an officer of the insurer for such term as APRA directs (s 97(1)(d));

(v) not to collect any premium (s 97(1)(g));

(vi) not to pay a dividend on any shares (s 97(1)(k);

(vii) to do, or refrain from doing, an act that relates to the way in which the affairs of the insurer are to be conducted or not conducted (s 97(1)(s));

(b) by written notice, to require the private health insurer to give APRA particular information, or a report, on particular matters, relating to the affairs of the insurer within the period specified in the notice (s 128(1));

(c) by written notice to the private health insurer or an officer of a private health insurer, to require the insurer or officer to produce to APRA any documents relating to the affairs of the insurer (s 129(1));

(d) to appoint an APRA staff member to be an inspector to investigate the affairs of a private health insurer if APRA reasonably suspects that (s 130(1)):

(i) the affairs of the insurer are being, or are about to be, carried on in a way that is not in the interests of the policy holders of a health benefits fund conducted by the insurer; or

(ii) the insurer has contravened an enforceable obligation;

(e) by written notice, from an inspector appointed under s 130 of the Private Health Supervision Act, to require that a person whom the inspector believes to have some knowledge of the affairs of the private health insurer that the inspector is investigating (s 132):

(i) produce to the inspector all or any documents relating to the affairs of the insurer that are in the custody, or under the control of, that person;

(ii) give to the inspector all reasonable assistance within the person's power in connection with the investigation; or

(iii) to appear before the inspector for examination concerning matters that are relevant to the investigation and are within the knowledge of the person;

(f) to accept a written undertaking given by a person in connection with a matter in relation to which APRA has a power or function under the Private Health Supervision Act (s 152(1)); and

(g) to apply to the Federal Court of Australia for a remedy specified in s 154(1) of the Private Health Supervision Act if APRA is satisfied that a private health insurer has contravened an enforceable obligation (s 154).

*B3.5 Risks posed by enforcement or other regulatory action*

71. At all times in the Relevant Period, Medibank was exposed to reputational risk by the existence of any actual or potential material non-compliance by Medibank and ahm with that entity's obligations under Australian Privacy Laws and applicable Prudential Standards.

72. At all times in the Relevant Period, Medibank was exposed to the Information Commissioner and APRA investigating whether to take, or taking, the steps referred to in paragraphs 68 to 70 above by the existence of any actual or potential material non-compliance by Medibank and ahm with that entity's obligations under Australian Privacy Laws and the applicable Prudential Standards.

73. At all times in the Relevant Period, Medibank was exposed to significant adverse financial effects by the existence of any:

(a) actual or potential material non-compliance by Medibank or ahm with its obligations under Australian Privacy Laws and the applicable Prudential Standards; and/or

(b) actual or potential vulnerabilities in the IT Systems Medibank had in place in respect of the Cyber Attack Risk.

**Particulars**

A. The financial impacts are additional costs and expenses, including fines, penalties, diverted management time, costs of external consultants (including lawyers), remediation, regulatory or litigation related costs or replacement costs, costs of complying with recommendations or directions made by the Office of the Australian Information Commissioner or the Information Commissioner (and applicable State or Territory counterparts), APRA or external third-party consultants, and additional or higher costs of capital associated with risks as pleaded in paragraphs 71 to 72 above.

B. Financial impacts incurred by Medibank Customers and ahm Customers cancelling or not renewing policies and/or decreased new policy purchases.

C. Further particulars may be provided following discovery.

## C. 2022 DATA BREACH

74. Multifactor authentication is and was at all times in the Relevant Period a well-known cybersecurity measure requiring two or more proofs of identity to grant access to a network or system.

75. At a point or points in time between about August 2022 and October 2022, one or more malicious cyber actors accessed Medibank's network:

(a) using the username and password of a Medibank contractor or employee; and

(b) without multifactor authentication, or without appropriately configured multifactor authentication.

**Particulars**

A. As to subparagraph (a), the plaintiffs do not presently know the identity of the malicious cyber actor or actors, the identity of the Medibank contractor or employee, the precise systems within Medibank's network accessed by malicious cyber actor or actors and the precise time of that access.

B. As to subparagraph (b), the plaintiffs do not presently know how the malicious cyber actor or actors accessed Medibank's network without multifactor authentication, although Medibank has said in its "Cyber event

timeline" (updated 23 February 2023) that "[t]he criminal used the stolen credentials to access Medibank's network through a misconfigured firewall which did not require an additional digital security certificate".

C. Further particulars may be provided following discovery.

76. Malicious cyber actors were thereafter able to obtain further Medibank usernames and passwords.

**Particulars**

The plaintiffs do not presently know which further usernames and passwords were obtained or when precisely they were obtained. The plaintiffs refer to Medibank's "Cyber event timeline" (updated 23 February 2023) and to the statement therein that "[t]he criminal was able to obtain further usernames and passwords to gain access to a number of Medibank's systems and their access was not contained".

77. Once malicious cyber actors had accessed Medibank's network, they extracted a substantial volume of data from Medibank's network, including the personal and health claims data of customers (**Stolen Customer Data**).

78. On or before 9 November 2022, malicious cyber actors released some of the Stolen Customer Data via the dark web.

79. By 1 December 2022, at least most of the Stolen Customer Data had been released by malicious cyber actors via the dark web.

## D. MEDIBANK'S REPRESENTATIONS TO THE MARKET

### D1. Medibank's statements

*D1.1 Medibank's 2016 statements*

80. On or about 19 August 2016, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2016 (**FY16 Financial Report**).

81. In the FY16 Financial Report, Medibank made the following statement:

(a) "Medibank may be affected by cyber-attacks or a failure in critical data, processes or systems. IT controls are continually under review and are protected through the use of detective, preventative and response tools" (p 6).

82. On or about 5 September 2016, Medibank published and lodged with the ASX its 2016 Annual Report (**2016 Annual Report**).

83. In the 2016 Annual Report, Medibank made the following statements:

(a) "Medibank may be affected by cyber-attacks or failure in critical data, processes or systems. IT controls are continually under review and are protected through the use of detective, preventative and response tools." (p 10);

(b) "The Audit and Risk Management Committee provides a non-executive review of the effectiveness of Medibank's financial reporting and risk management framework, and assists the Board in carrying out its accounting, auditing, risk management, regulatory compliance and financial reporting responsibilities." (p 23);

(c) "Medibank maintains a system of risk oversight, risk management and internal control over material business risks, including the accuracy of financial reporting. This is designed to provide reasonable assurance of the implementation of the Board's financial reporting policies, the integrity of the Group's financial reporting and management of its material business risks within the Board- approved risk appetite." (p 24);

(d) "The Board has overall responsibility for Medibank's risk management framework including setting the risk management policy and determining the risk appetite for Medibank. The Board reviews, at least annually, the policies and procedures on risk oversight and management and satisfies itself that management has developed and implemented a sound system of risk management and internal control to meet prudential and statutory requirements. The Audit and Risk Management Committee assists the Board in setting the risk management policy and appetite and monitoring whether the business is operating within the limits set. The committee performs a detailed review, at least annually, of the risk management system to ascertain whether it effectively manages material business risks and is operating effectively in relation to financial reporting risks. If required, the committee considers reports concerning material risk events and incidents and oversees their resolution by management." (p 24); and

(e) "The risk management framework sets out clearly-defined criteria to analyse, evaluate and prioritise material business risk. This includes systematically assessing risk consequences in terms of impact upon clinical governance, employee safety, regulatory, legal, financial, shareholder, reputation, operations and business performance. During 2016 the Board assessed the risk management framework and concluded that the material risks are within the overall risk appetite but there remains scope for further mitigation and improvement. The current focus is to more closely

align, where appropriate, Medibank's risk management framework with that prescribed by APRA for the general insurance industry, as the regulation of the private health insurance industry transitions to APRA from the Private Health Insurance Administration Council." (p 24).

*D1.2 Medibank's 2017 statements*

84. On or about 25 August 2017, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2017 (**FY17 Financial Report**).

85. In the FY17 Financial Report, Medibank made the following statement:

(a) "Medibank may be affected by cyber-attacks or failure in critical data, processes or systems. IT controls are continually under review and are protected through the use of detective, preventative and response tools." (p 7).

86. On or about 12 September 2017, Medibank published and lodged with the ASX its 2017 Annual Report (**2017 Annual Report**).

87. In the 2017 Annual Report, Medibank made the following statements:

(a) "Medibank may be affected by cyber-attacks or failure in critical data, processes or systems. IT controls are continually under review and are protected through the use of detective, preventative and response tools." (p 11);

(b) "Medibank maintains a system of risk oversight, risk management and internal control over material business risks, including accuracy of financial reporting. This is designed to provide reasonable assurance of the implementation of the Board's financial reporting policies, the integrity of the Group's financial reporting and management of its material business risks within the Board-approved risk appetite." (p 26);

(c) "During 2017, management revised the risk management framework to more closely align with APRA Prudential Standard CPS 220 – Risk Management. This process will continue in the coming year in the lead up to that standard being applied to the private health insurance industry from 1 April 2018." (p 27);

(d) "The Board has overall responsibility for Medibank's risk management framework including determining the risk appetite for Medibank. The Board reviews the risk framework at least annually and satisfies itself that management has developed and implemented a sound system of risk management and internal control to meet

prudential and statutory requirements. The Board reviewed the risk management framework during 2017 and concluded that it is sound." (p 27);

(e) "The newly established Risk Management Committee assists the Board in setting the risk appetite and monitoring whether the business is operating within the limits set." (p 27);

(f) "Medibank has a three lines of defence approach to risk management accountability. First line: Management is accountable for identifying, assessing, monitoring and managing material risks in the business. They are responsible for decision making and the execution of business activities, whilst managing risk to ensure it is in line with the board's risk appetite and strategy. Second line: The Enterprise Risk function provides objective advice and challenge to the first line on risk and control activities and provides assurance and guidance on the design and implementation of appropriate risk management activities. To ensure the independence of the risk function, the Chief Risk Officer reports (with a dotted line) to the Chair of the Risk Management Committee. Third line: Internal Audit provides independent assurance to the Audit Committee and the Board on the adequacy and effectiveness of the risk management framework, financial reporting processes and internal control and compliance systems operating at the first and second line." (p 27); and

(g) "Medibank's risk management framework sets out clearly-defined criteria to analyse, evaluate and prioritise material business risks. This includes systematically assessing risk consequences in terms of impact upon clinical governance, employee health and safety, financial performance and position, regulatory and legal obligations, reputation and operations." (p 27).

*D1.3 Medibank's 2018 statements*

88. On or about 24 August 2018, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2018 (**FY18 Financial Report**).

89. In the FY18 Financial Report, Medibank made the following statement:

(a) "Medibank has established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud and people risks. Management of operational risk is overseen by Divisional Risk

Committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 9).

90. On or about 17 September 2018, Medibank published and lodged with the ASX its 2018 Annual Report (**2018 Annual Report**).

91. In the 2018 Annual Report, Medibank made the following statements:

(a) "Medibank has established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud and people risks. Management of operational risk is overseen by Divisional Risk Committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 24);

(b) "Key areas of focus for the board in 2018 - Oversight of the implementation of APRA Prudential Standard CPS 220 compliant risk management framework – Review of material risks and opportunities and emerging risks, and strengthening of risk culture throughout the organisation" (p 32);

(c) "Medibank's Risk Management Framework encompasses the systems, structures, policies, processes and people that manage risks across the business. It guides risk management activities across the business to effectively identify, assess, manage, monitor and report risks. The framework is implemented through the three lines of defence model and its effectiveness is assessed by the internal audit function on an annual basis. A key component of the framework is the definition of Medibank's risk appetite by the Board which informs management's decision making process. Over the last twelve months, Medibank invested significant resources to strengthen the enterprise risk management practices to ensure alignment with the requirements outlined in the APRA Prudential Standard CPS220 – Risk Management which became applicable to the private health insurance industry on 1 April 2018." (p 41);

(d) "The Board has overall responsibility for Medibank's Risk Management Framework including setting the risk appetite for Medibank. The Board reviews the risk framework at least annually and satisfies itself that management has developed and implemented a sound system of risk management and internal control to effectively manage risk across the business in line with regulatory and statutory requirements. The Board reviewed the risk management framework during 2018 and concluded that it is sound." (p 41); and

(e) "Medibank has adopted a three lines of defence approach to define risk management roles, responsibilities and accountability. First line: Management is accountable for identifying, assessing, monitoring and managing material risks in the business. They are responsible for decision making and the execution of business activities, whilst managing risk to ensure it is in line with the Board's risk appetite and strategy. Second line: The Enterprise Risk and Compliance functions provides objective advice and challenge to the first line on risk and control activities and provides assurance and guidance on the design and implementation of appropriate risk management activities. Third line: Internal Audit provides independent assurance to the Audit Committee and the Board on the adequacy and effectiveness of the risk management framework, financial reporting processes and internal control and compliance systems operating at the first and second line." (p 41).

*D1.4 Medibank's 2019 statements*

92. On or about 22 August 2019, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2019 (**FY19 Financial Report**).

93. In the FY19 Financial Report, Medibank made the following statement:

(a) "Medibank has established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 9).

94. On or about 17 September 2019, Medibank published and lodged with the ASX its 2019 Annual Report (**2019 Annual Report**).

95. In the 2019 Annual Report, Medibank made the following statements:

(a) "Our customers trust us with their personal health information and maintaining that trust through our security and governance systems to protect that data remains our priority." (p 8);

(b) "Medibank has established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud and people risks. Management of operational risk is overseen by divisional risk

committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 28);

(c) "the Board has identified as critical enablers skills in human resources and remuneration and technology and has ensured that the Board has covered these areas of expertise in constituting the current Board." (p 36);

(d) "Key areas of focus for the Board in 2019 - Oversight of the implementation of the enterprise risk and compliance management framework, including the effectiveness of the risk management framework which is aligned with the APRA Prudential Standard CPS 220 - Review and monitoring of financial and non-financial material risks and emerging risks." (p 35);

(e) "Medibank's risk management framework encompasses the systems, structures, policies, processes and people that manage risks across the business. It guides risk management activities across the business to effectively identify, assess, manage, monitor and report risks. The framework is implemented through the three lines of defence model and its effectiveness is assessed by the internal audit function on an annual basis in accordance with the Risk Management Committee Charter. A review of the framework was completed for 2019." (p 43);

(f) "Over the last 12 months, Medibank has continued to strengthen enterprise risk management practices in alignment with the requirements outlined in the APRA Prudential Standard CPS220 – Risk Management." (p 43);

(g) "The Board has overall responsibility for Medibank's risk management framework including setting the risk appetite for Medibank. The Board reviews the risk management framework at least annually and satisfies itself that management has developed and implemented a sound system of risk management and internal control to effectively manage risk across the business in line with regulatory and statutory requirements." (p 43); and

(h) "Medibank has adopted a three lines of defence approach to define risk management roles, responsibilities and accountability. First line: Management is accountable for identifying, assessing, monitoring and managing material risks in the business. They are responsible for decision making and the execution of business activities, whilst managing risk to ensure it is in line with the Board's risk appetite and strategy. Second line: The enterprise risk and compliance functions provide objective advice and challenge to the first line on risk and control activities and provide assurance and

guidance on the design and implementation of appropriate risk management activities. Third line: The internal audit function provides independent assurance to the Audit Committee and the Board on the adequacy and effectiveness of the risk management framework, financial reporting processes and internal control and compliance systems operating in the first and second line." (p43).

*D1.5 Medibank's 2020 statements*

96. On or about 20 August 2020, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2020 (**FY20 Financial Report**).

97. In the FY20 Financial Report, Medibank made the following statement:

    (a) "Medibank has established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 8).

98. On or about 10 September 2020, Medibank published and lodged with the ASX its 2020 Annual Report (**2020 Annual Report**).

99. In the 2020 Annual Report, Medibank made the following statements:

    (a) "Medibank has established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 28);

    (b) "Material topics - … Privacy and data security." (p 20);

    (c) "Oversight of the enhancement of the enterprise risk and compliance management framework and risk and compliance culture, including review and monitoring of financial and non-financial material risks and emerging risks and the coordination of the first review by the Appointed Auditor as required by APRA Prudential Standard CPS510." (p 36);

(d) "Medibank's risk management framework encompasses the systems, structures, policies, processes and people that manage risks across the business. It guides risk management activities across the business to effectively identify, assess, manage, monitor and report risks. The framework is implemented through the three lines of defence model and its effectiveness is assessed by the internal audit function on an annual basis in accordance with the Risk Management Committee Charter. A review of the framework was completed for 2020." (p 44);

(e) "Medibank continues to operate and strengthen enterprise risk management practices in alignment with the requirements outlined in the APRA Prudential Standard CPS220 – Risk Management." (p 44); and

(f) "Medibank has adopted a three lines of defence approach to define risk management roles, responsibilities and accountability. First line: Management is accountable for identifying, assessing, monitoring and managing material risks in the business. They are responsible for decision making and the execution of business activities, whilst managing risk to ensure it is in line with the Board's risk appetite and strategy. Second line: The enterprise risk and compliance functions provide objective advice and challenge to the first line on risk and control activities and provide assurance and guidance on the design and implementation of appropriate risk management activities. Third line: The internal audit function provides independent assurance to the Audit Committee and the Board on the adequacy and effectiveness of the risk management framework, financial reporting processes and internal control and compliance systems operating in the first and second line." (p 44).

100. On or about 10 September 2020, Medibank published its 2020 Sustainability Report on its website (**2020 Sustainability Report**).

**Particulars**

To the best of the plaintiff's knowledge prior to discovery, the 2020 Sustainability Report was published on or about 10 September 2020: "A year in review – Medibank in 2020" (10 September 2020) https://www.medibank.com.au/livebetter/newsroom/post/a-year-in-review-medibank-in-2020 (accessed 29 June 2023). The 2020 Sustainability Report was published in the "Investor Centre" section of Medibank's website, alongside Medibank's 2020 Annual Report.

101. In the 2020 Sustainability Report, Medibank made the following statements:

(a) "our material topics … Privacy and data security. Protect our customers' privacy through secure systems and processes." (p 4);

(b) "our material topics … Corporate governance. Effectively manage risk and maintain legislative and regulatory compliance." (p 4);

(c) "Protect our customers' privacy through secure systems and processes. Our customers trust us with their personal information. Maintaining that trust by managing and protecting that information in accordance with customer expectations and our legal obligations is a priority for everyone in Medibank. We do this by taking a holistic, risk-based approach embedded within our privacy, cybersecurity, risk management, assurance and information management frameworks, systems, policies and processes." (p 14);

(d) "Keeping data secure. Our Cybersafety Policy is based on an information-centric, risk-based approach that aligns the protection of information with our business strategy and regulatory obligations. We have well-defined, good practice data management policies and processes, supported by employee training and systems that make effective data management part of our day-to-day work practices." (p 14);

(e) "How we store data. Our security controls are applied across our IT environment, whether hosted in our private data centre or cloud provider. We expect appropriate levels of controls be applied to all assets, regardless of location, and we implement multiple security controls commensurate with the sensitivity of the data itself." (p 14);

(f) "In addition to the security controls we've embedded within our systems, platforms and processes, we have implemented a standards-based, industry-accepted good practice security framework covering all aspects of security governance, risk, audit, compliance and reporting, that is closely aligned to the National Institute of Standards and Technology (NIST) Cyber Security Framework. Our compliance with APRA's CPS234 Information Security standard complements our security approach". (p 14);

(g) "How we handle data privacy breaches. Our enterprise governance, risk and compliance management processes help us identify and manage privacy and data security risks and incidents." (p 14);

(h) "We work with our employees to detect, contain, assess, respond to and, where necessary, notify any data breaches which occur, as well as to respond to any privacy

concerns or complaints we receive from our customers. We take the learnings from these experiences to continually improve our processes and meet our privacy compliance obligations under the Australian Privacy Principles (APP) and Australian Mandatory Data Breach Notification (MDBN) legislation." (p 14);

(i) "Educating our people about information privacy and security. We believe everyone has a part to play in protecting the privacy and security of information. We strive to create a culture of privacy and security awareness across all of Medibank, through an ongoing program of privacy and cybersecurity awareness education and training, in addition to regular compliance training. We also conduct targeted role-based training and education for teams, focused on people in roles that deal directly with customer information such as our retail and customer support teams." (p 14);

(j) "Compliance. To help our people understand our regulatory obligations and how they apply in their role, all our employees complete a number of compulsory learning modules each year in areas such as privacy…" (p 43);

(k) "Effectively manage risk and maintain legislative and regulatory compliance. Our Board is committed to sound corporate governance practices which ensure it meets its obligations and responsibilities to the company, its shareholders and stakeholders. It has established a framework of adopting internal controls, risk and compliance management processes and corporate governance policies and practices, designed to promote responsible management and ethical conduct." (p 44);

(l) "Risk culture. Our risk management framework encompasses the systems, structures, policies, processes and people that manage risks across the business. It guides our risk management activities across the business to effectively identify, assess, manage, monitor and report risks. It is implemented through the three lines of defence model and its effectiveness is assessed annually, by the internal audit function, in accordance with the Risk Management Committee Charter. A key component is Medibank's risk appetite as defined by the Board, more details of which can be found in our 2020 Annual Report." (p 45); and

(m) "The management of financial and non-financial risks by senior executives is reviewed by the Risk Management Committee, which considers the effective operation of the Executive Risk Committee, incident identification, audit findings, risk and compliance remediation actions, and the results from our My Voice employee surveys regarding health and safety and risk culture. In addition, our Chief Risk

Officer and Group Executive – Legal, Governance & Regulatory Affairs are responsible for notifying the Board of any relevant risk and compliance outcomes and/or conduct which may impact the performance and remuneration outcomes for Executive Leadership Team members and other senior executives." (p 45).

*D1.6 Medibank's 2021 statements*

102. On or about 25 August 2021, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2021 (**FY21 Financial Report**).

103. In the FY21 Financial Report, Medibank made the following statement:

(a) "We have established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 8).

104. On or about 17 September 2021, Medibank published and lodged with the ASX its 2021 Annual Report (**2021 Annual Report**).

105. In the 2021 Annual Report, Medibank made the following statements:

(a) "We have established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 28);

(b) "The [risk management] framework is implemented through the three lines of defence model and its effectiveness is assessed by the internal audit function on an annual basis with a full comprehensive review on a three yearly basis in accordance with the Risk Management Committee Charter and APRA Prudential Standard CPS220, with these reports being provided to and reviewed by the Risk Management Committee. Both annual and three yearly reviews of the framework were completed in 2021. The Risk Management Committee reviews the documents comprising the risk management framework at least yearly and regularly monitors the framework's effectiveness." (p 46); and

(c) "Medibank has adopted a three lines of defence approach to define risk management roles, responsibilities and accountability: First line: Management is accountable for identifying, assessing, monitoring and managing material risks in the business. They are responsible for decision making and the execution of business activities, whilst managing risk to ensure it is in line with the Board's risk appetite and strategy. Second line: The enterprise risk and compliance functions provide objective advice and challenge to the first line on risk and control activities and provide assurance and guidance on the design and implementation of appropriate risk management activities. Third line: The internal audit function provides independent assurance to the Audit Committee and the Board on the adequacy and effectiveness of the risk management framework, financial reporting processes and internal control and compliance systems operating in the first and second line." (p 46).

106. On or about 17 September 2021, Medibank published its 2021 Sustainability Report on its website (**2021 Sustainability Report**).

**Particulars**

To the best of the plaintiff's knowledge prior to discovery, the 2021 Sustainability Report was published on or about 17 September 2021: "Creating a sustainable future – a look back on FY21" (17 September 2021) https://www.medibank.com.au/livebetter/newsroom/post/creating-a-sustainable-future-a-look-back-on-fy21 (accessed 29 June 2023). The 2021 Sustainability Report was published in the "Investor Centre" section of Medibank's website, alongside Medibank's 2021 Annual Report.

107. In the 2021 Sustainability Report, Medibank made the following statements:

(a) "Our material topics … Privacy and data security. Protect our customers' privacy through secure systems and processes." (p 4);

(b) "Protect our customers' privacy through secure systems and processes. As a health company, we take seriously our responsibility to manage and protect our customers' and employees' information and privacy, working to ensure the security of our services and operations. It's what our customers and the community expect of us." (p 19);

(c) "Educating our employees. Our people are our first line of defence – they are key to helping us protect the information we hold. We regularly educate our employees throughout the year, in addition to our annual compulsory privacy and data protection training that all our people undertake." (p 19);

(d) "Retail and customer support team members along with others who deal with customer information also receive additional role-based training. It's part of our culture to know and care about protecting the information we use." (p 19);

(e) "Our commitment to privacy. We aim for strong, effective and contemporary privacy management practices and systems that will enhance trust and confidence in the way that we do business. This year we developed a Privacy Framework to guide our approach, that focuses on these key principles.

1. Creating a culture of privacy awareness.

2. Recognising that we handle sensitive information and manage diverse operations across our business, and we take a responsible approach to ensuring that privacy is respected.

3. Integrating privacy into our enterprise risk, compliance and incident management systems.

4. Applying a risk-based approach to privacy and encouraging open, proactive conversations about privacy risk.

5. Embedding privacy practices.

6. Expecting a high degree of best practice privacy compliance from our employees and our systems.

We're committed to providing our customers with transparency in relation to how we collect, store and use their data. Our Privacy Policy is available online and provides details on:

• our collection, use and disclosure of information

• how customers can access their personal information

• when and how we dispose of personal information." (p 19);

(f) "Keeping information secure. From the way we manage mobile devices to our malware protection, security monitoring and incident responses, our risk-based approach ensures that information security and privacy practices are part of our day-to-day activity. Our approach is strongly embedded across our business processes, policies, systems and frameworks. We conduct privacy impact assessments when needed on services, projects or procurement of services that involve personal and

sensitive information. We also have disaster recovery plans in place which detail the response and recovery steps and timeframes required, should an incident occur. We regularly verify our information security controls in annual Payment Card Industry Data Security Standard (PCI DSS) compliance audits as well as internal and external audit programs." (p 20);

(g) "How we store and use personal information. We apply security controls across all of our IT environment, including our data centres, software and applications, mobile devices and physical locations. These controls reflect the sensitivity of the data being protected, and we test our systems regularly. Our processes also help ensure information is only accessible to those employees who require access for their role, and we review our employees' system access regularly." (p 20);

(h) "How we handle data breaches or security incidents. We work across teams to identify and manage any privacy or information security risks that may occur. In the event of a breach, our incident response process is designed to enable us to respond quickly – first determining the severity of the incident before enacting our established response plans so we can limit the impact and resolve the issue. As part of our incident management process, every security incident is subject to a post incident review (PIR) from which we take detailed learnings to adapt our incident process as required." (p 20);

(i) "We continue optimising our IT security incident response capabilities, through our partnerships with major government agencies and cybersecurity organisations. We draw on their deep technical capabilities to deliver in-depth, tailored security incident response simulations to assess our cyber resilience. We also ensure that we meet all our privacy compliance obligations under the Australian Privacy Principles (APP)." (p 20);

(j) "Adopting best practice. Our approach to data security has been guided by the Cyber Security Framework developed by the National Institute of Standards and Technology. We also draw upon best practices and controls from other international standards and frameworks including the ISO 27001, Australian Signals Directorate and Australian Prudential Regulation Authority. We ensure we're compliant with national laws and regulations and keep updated on global privacy and data protection laws and regulations. Our cyber risk and security control capabilities and training programs are also audited regularly by independent internal and external teams and we use the

learnings from any incidents that occur to help us continuously improve our processes." (p 21);

(k) "Case study. Testing our readiness and resilience. Each year we test our readiness for managing cybersecurity incidents running a number of simulation exercises to assess our resilience, across the business involving teams from technology and operations, legal, privacy, compliance, risk management, external affairs, marketing and members of our senior leadership team. Each simulation aims to review our plans and procedures when responding to a significant cybersecurity event – how we deal with the threat, recover from any loss and/or damage to our systems and services and manage reputational damage. This year, our simulations included common ransomware attacks impacting Medibank or a member of our supply chain or both. The lessons we learn from these exercises are then integrated into our response training program, to support the continued improvement of our security capabilities." (p 21);

(l) "Effectively manage risk and maintain legislative and regulatory compliance. To meet our responsibilities and obligations to our shareholders, stakeholders and employees, the Board has instigated a framework of corporate governance policies and practices, internal controls, and risk and compliance management processes. These are designed to promote responsible management and ethical conduct." (p 60);

(m) "Risk culture. Our strong purpose-led culture and values help to guide the behaviours we expect of our people. This is further supported by our risk culture approach, which details what is expected of our team members to ensure we're not only complying with our legal obligations, but we're acting ethically and responsibly. Our risk management framework is designed to effectively identify, assess, manage, monitor and report risks." (p 61);

(n) "Overall responsibility is held by the Board, including setting the risk appetite for Medibank. We use a three lines of defence approach to define risk management roles, responsibilities and accountability. The management of financial and non-financial risks by senior executives is reviewed by the Risk Management Committee, and our internal audit team assesses the effectiveness of our risk management, in accordance with our Risk Management Committee Charter." (p 61);

(o) "We have established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing,

fraud, people, and health and safety risks. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 62); and

(p) "We have established compliance management policies and procedures for identifying and managing Medibank's regulatory obligations and incidents that may arise. Management of compliance risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 63).

*D1.7 Medibank's 2022 statements*

108. On or about 18 August 2022, Medibank published and lodged with the ASX its Appendix 4E Financial Report for the Financial Year ending 30 June 2022 (**FY22 Financial Report**).

109. In the FY22 Financial Report, Medibank made the following statement:

(a) "We have established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. We have established compliance management policies and procedures for identifying and managing regulatory obligations and incidents that may arise. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 8).

110. On or about 15 September 2022, Medibank published and lodged with the ASX its 2022 Annual Report (**2022 Annual Report**).

111. In the 2022 Annual Report, Medibank made the following statements:

(a) "We've also strengthened our privacy and data security capabilities and requirements to ensure our customers are better protected." (p 9);

(b) "We have established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. We have established compliance management policies and procedures for identifying and managing regulatory obligations and incidents that may arise. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee." (p 28);

(c) "Requires directors, managers, employees and contractors to behave with high standards of personal integrity, and in a manner that: … respects privacy and protects confidential information." (p 42);

(d) "Oversight of the enhancement of the enterprise risk and compliance management framework and risk and compliance culture, including review and monitoring of financial and non-financial material risks and emerging risks." (p 36);

(e) "Medibank's risk management framework encompasses the systems, structures, policies, processes and people that manage risks across the business. It guides risk management activities across the business to effectively identify, assess, manage, monitor and report risks. The framework is implemented through the three lines of defence model and its effectiveness is assessed by the internal audit function on an annual basis with a full comprehensive review on a three yearly basis in accordance with the Risk Management Committee Charter and APRA Prudential Standard CPS220. The annual review of the framework was completed in 2022, with the three yearly comprehensive review having been undertaken in 2021. The Risk Management Committee reviews the documents comprising the risk management framework at least yearly and regularly monitors the framework's effectiveness." (p 47); and

(f) "Medibank has adopted a three lines of defence approach to define risk management roles, responsibilities and accountability: First line: Management is accountable for identifying, assessing, monitoring and managing material risks in the business. They are responsible for decision making and the execution of business activities, whilst managing risk to ensure it is in line with the Board's risk appetite and strategy. Second line: The enterprise risk and compliance functions provide objective advice and challenge to the first line on risk and control activities and provide assurance and guidance on the design and implementation of appropriate risk management activities. Third line: The internal audit function provides independent assurance to the Audit Committee and the Board on the adequacy and effectiveness of the risk management framework, financial reporting processes and internal control and compliance systems operating in the first and second line." (p 47).

112. On or about 15 September 2022, Medibank published its 2022 Sustainability Report on its website (**2022 Sustainability Report**).

**Particulars**

To the best of the plaintiff's knowledge prior to discovery, the 2022 Sustainability Report was published on or about 15 September 2022: "Creating a healthier future for all Australians" (15 September 2022) https://www.medibank.com.au/livebetter/newsroom/post/creating-a-healthier-future-for-all-australians (accessed 29 June 2023). The 2022 Sustainability Report was published in the "Investor Centre" section of Medibank's website, alongside Medibank's 2022 Annual Report.

113. In the 2022 Sustainability Report, Medibank made the following statements:

(a) "In 2020, we undertook an extensive materiality assessment that identified 16 material topics across five key pillars, which has guided our sustainability strategy and approach. As sustainability-related risk and opportunities become increasingly important to us and the ESG expectations of our stakeholders continue to evolve, we reassess our material topics regularly. This year, we reviewed our materiality assessment to examine the relevance of our existing topics in meeting our stakeholders' and our own expectations and to identify any gaps that might exist. Working with our partner, we undertook interviews with external and internal stakeholders, a customer insights survey, peer benchmarking and an analysis of our current strategy." (p 4);

(b) "Our material topics. Corporate and clinical governance. Privacy and data security." (p 5);

(c) "The issues that matter - Ethical and sustainable business - How we're enabling this - Corporate and clinical governance - Privacy and data security." (p 61);

(d) "Corporate governance. Our Board has instigated a framework of corporate governance policies and practices, internal controls, and risk and compliance management processes to meet our responsibilities and obligations to our customers and patients, employees, shareholders and stakeholders, and promote responsible management and ethical conduct. Five standing Board committees have been established to assist the Board in managing its corporate governance responsibilities. Each is governed by a charter setting out the committee's role, responsibilities, membership and processes – more detail on which is available on our website. The Medibank Board holds overall responsibility for sustainability and corporate responsibility issues, while other Board committees have input into environmental, social and governance issues." (p 64);

(e) "Executive Risk Committee and Divisional Risk committees. Oversees, directs and supports the implementation and operation of Medibank's risk and compliance management framework – including financial and non-financial risks." (p 64);

(f) "Through our risk management framework, we aim to effectively identify, assess, manage, monitor and report risks. Overall responsibility for risk, including setting the risk appetite for Medibank, is held by the Board. We use a three lines of defence approach to define risk management roles, responsibilities and accountability. The management of financial and non-financial risks by senior executives is reviewed by the Risk Management Committee, and our Enterprise Risk and Group Compliance functions provide oversight of the effectiveness of risk management practices. In addition, our internal audit team regularly assesses the effectiveness of risk management in accordance with our Risk Management Committee Charter." (p 65);

(g) "Emerging risks we are tracking include a heightened cyber risk associated with the geo-political environment, the ongoing impact of COVID on talent and resource availability, wage price growth in the Australian economy as well as the impacts on the global economy from COVID and economic sanctions caused by geo-political tensions." (p 65);

(h) "We have established risk management policies and procedures for identifying, assessing, monitoring and reporting operational risks and controls. This includes the important areas of information security, technology, business continuity, outsourcing, fraud, people, and health and safety risks. We also have established compliance management policies and procedures for identifying and managing regulatory obligations and incidents that may arise. Management of operational risk is overseen by divisional risk committees, the Executive Risk Committee and the Board's Risk Management Committee" (p 66);

(i) "Emerging risk (including ESG risk) - Heightened cyber risk associated with the geo-political environment" (p 67);

(j) "Privacy and data security. As a health company, we are trusted with managing and protecting our customers' and employees' information and privacy and have a responsibility to ensure our services and operations are secure. Our privacy framework has been designed to enhance trust and confidence in the way we do business through strong, effective and contemporary privacy management practices and systems centred on six key principles." (p 69);

(k) "Fostering and maintaining a culture of privacy awareness • Recognising that we handle sensitive information and manage diverse operations across our business, and we take a responsible approach to ensuring that privacy is respected • Integrating privacy into our enterprise risk, compliance and incident management systems • Applying a risk-based approach to privacy and encouraging open, proactive conversations about privacy risk • Embedding good privacy practices • Expecting a high degree of best practice privacy compliance from our employees and our systems." (p 69);

(l) "Being open about privacy. We've continued reviewing and improving our Privacy Policy and practices to make it easier for customers to understand how we collect, store and use their data. Our policy is available online and also includes details on how we dispose of information and how people can access their personal information. We also seek consent upfront and provide notices regarding personal information where required." (p 69);

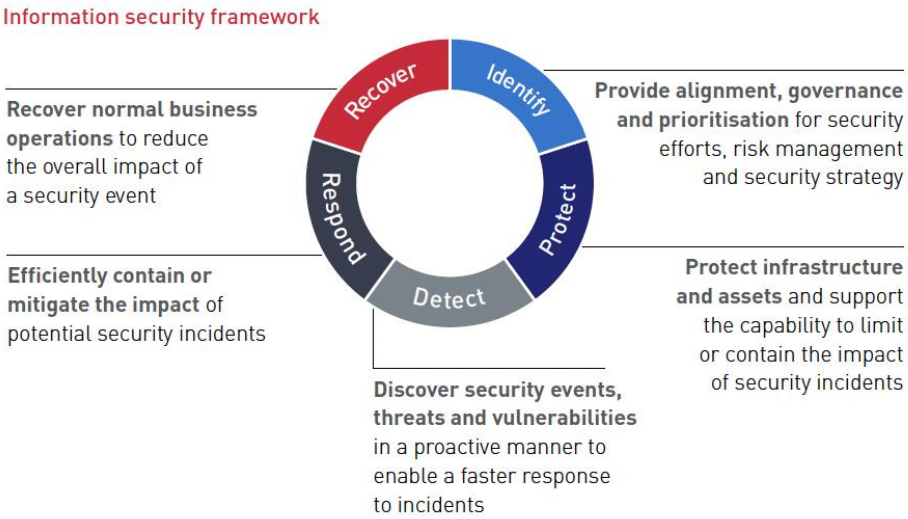
(m) "Keeping information safe. Information security and privacy practices are embedded into our day-to-day activities and applied through our business processes, policies, systems and frameworks. We continue strengthening our privacy and data security foundations to ensure we can adapt and rapidly respond to changing and increasingly complex digital/ cyber environments. This year, we established a new security operations centre with a broader responsibility, more specialised roles and enhanced tools. We further enhanced our security capabilities enabling our people to work flexibly from any location. We also took greater advantage of security automation to increase the number of risk assessments of third-party vendors conducted before they started working on a project or service. We repeatedly test for any vulnerabilities that might exist across our systems and maintain detailed disaster recovery plans that we review and update regularly. Independent internal and external teams conduct regular audits of our cyber risk and security control capabilities, including annual Payment Card Industry Data Security Standard (PCI DSS) compliance audits. We also do privacy impact assessments on services, projects or procurement of services that involve personal and sensitive information when needed." (p 69);

(n) "Best-in-class approach. Our cyber security approach is guided by the National Institute of Standards and Technology's Cyber Security Framework and draws upon best practices and controls from other international standards and frameworks including the ISO 27001, Australian Signals Directorate and Australian Prudential

Regulation Authority. We're compliant with national laws and regulations and keep updated on global privacy and data protection laws and regulations. Over the next 12 months, we'll be reviewing our existing security model to identify opportunities to further enhance how we keep our customers' data secure and private, and secure our systems and processes as we continue to grow as a health company." (p 70);

(o) "Case study. Delivering our vision on a foundation of trust Protecting people's data and respecting privacy is central to what we're doing to build more personalised and connected health and wellbeing experiences for our customers. Our customers want health support tailored to their own needs and a health system that is easier to navigate and simpler to use. To deliver this, we will need to utilise information we have about our customers, and we want to be very open about how we will do this and ensure people can control their information. We value our customers' privacy rights. So, as we develop these new experiences, we will be embedding privacy and data controls that will enable appropriate mechanisms to protect and respect customers' privacy rights – including their right to choose – and ensure their information is protected." (p 70);

(p) (at p 70):




(q) "Building a cyber culture. Every one of our people is key to protecting the information we hold – they are our first line of defence against security threats. We've continued to invest in and enhance our cyber culture, this year surveying our people across the business to create a base profile for security culture. We regularly educate our people, including using informal channels to offer helpful security information applicable to

people's daily lives. We also require employees to undertake training throughout the year, including compulsory privacy and data protection training, to ensure they understand the role they play in keeping information safe." (p 71);

(r) "How we store and use information. Security controls reflecting the sensitivity of the data being protected are applied across all of our IT environment. This includes our data centres, software and applications, mobile devices and physical locations and we test our systems regularly. We also ensure that information is only accessible to those employees who require access for their role, and we review our employees' system access regularly." (p 71); and

(s) "Managing security incidents or data breaches. Our incident response process enables us to respond quickly should a situation occur. It brings together the required teams from across the business to first determine how severe a breach is and then to enact our established response plans to limit any impact and resolve the issue. Following any incident, we hold a review, from which we take detailed learnings to adapt our process as required. We draw upon our relationships with major government agencies and cybersecurity organisations to both inform and test our cybersecurity resilience and run regular simulations. We also ensure that we meet all our privacy compliance obligations under the Australian Privacy Principles (APP)." (p 71).

*D1.8 Medibank's statements in its Privacy Policies*

114. On a date presently unknown to the plaintiffs, Medibank published a document entitled '"Medibank Privacy Policy May 2015"' on its website (**2015 Privacy Policy**).

115. In the 2015 Privacy Policy, Medibank made the following statements:

(a) "We are committed to protecting your personal information and complying with our obligations under the *Privacy Act 1988* (Cth) (Privacy Act) and other State and Territory laws governing the use of personal information (collectively, Privacy Laws) which regulate how personal information is handled from collection to use and disclosure, storage, access and disposal." (p 2);

(b) "We take all reasonable steps to protect your personal information from misuse and loss and from unauthorised access, modification or disclosure. We store your information securely and have a range of security controls in place to ensure that your information and documents are protected. Our employees are trained on privacy and

access to personal information is restricted to individuals properly authorised to do so." (p 4); and

(c) "We keep your personal information for only as long as it is required in order to provide you with products and services and to comply with our legal obligations. When it is no longer needed for these purposes, we take reasonable steps to destroy or permanently de-identify this personal information." (p 4).

**Particulars**

A. A copy of the 2015 Privacy Policy as at about 6 April 2019 is in the possession of the plaintiffs' solicitors and may be inspected by request.

B. Further particulars may be provided following discovery.

116. On a date presently unknown to the plaintiffs, Medibank published on its website a web page entitled "Privacy Policy" (**Privacy Web Text**).

117. In the Privacy Web Text, Medibank made the following statements:

(a) "We are bound by laws governing how we collect and use your personal information including the Privacy Acy 1988 (Cth) and other State and Territory laws such as the Health Records Act 2001 (Vic), Health Records (Privacy and Access) Act 1997 (ACT), the Health Records and Information Privacy Act 2002 (NSW), and the Health Information Privacy Code 1994 in New Zealand …"

(b) "How we hold your personal information. We aim to store your information securely and have a range of security controls in place (including physical, technical and procedural safeguards) designed to protect your personal information. Our employees and contractors regularly receive targeted privacy training. We take reasonable steps to make sure that the personal information about you – that we collect, use and disclose, is accurate, complete, up to date and relevant.";

(c) "When and how we dispose of your personal information. We seek to keep your personal information for only so long as it is required in order to provide you with products and services or to legitimately comply with our business and legal obligations and requirements. When it is no longer needed for these purposes, we may destroy or permanently de-identify this personal information …"; and

(d) "De-identifying your information. Where possible and in our view – appropriate, where using your personal information, we will seek to de-identify it, so that your

identity is not readily ascertainable from the de-identified information or from triangulating your de-identified information with other sources of information".

**Particulars**

A. A copy of the Privacy Web Text as at about 29 February 2020 is in the possession of the plaintiffs' solicitors and may be inspected by request.

B. Further particulars may be provided following discovery.

## D2. Medibank's Representations

### *D2.1 Medibank's CPS 234 Compliance Representation*

118. By reason of the matters pleaded in paragraph 101(f) above, on 10 September 2020, Medibank represented to the market of investors and potential investors in MPL Shares (**Affected Market**) that it complied with CPS 234 (**Medibank's CPS 234 Compliance Representation**).

**Particulars**

The representation was express and was constituted by the statement: "Our compliance with APRA's CPS234 Information Security standard complements our security approach."

### *D2.2 Medibank's Cyber Security Representations*

119. On 10 September 2020, by reason of the matters pleaded in paragraphs 100 and 101 above, alternatively those matters pleaded in paragraphs 80 to 99 above, Medibank made the representations to the Affected Market pleaded in paragraphs 121 to 124 below.

**Particulars**

A. The representations were partly express and partly implied.

B. To the extent that they were express, the plaintiffs refer to:

1. the statements pleaded in paragraph 101 above;

2. in the alternative, those statements read in the context of the statements pleaded in paragraphs 81, 83, 85, 87, 89, 91, 93, 95, 97 and/or 99 above.

C. To the extent they were implied, they were implied by the statements referred to in B above and by the absence of Medibank making any statement that qualified or contradicted those statements.

120. In the alternative to paragraph 119, Medibank made those representations to the Affected Market:

(a) on 25 August 2021, by reason of the matters pleaded in paragraphs 100 to 103 above;

(b) on 17 September 2021, by reason of the matters pleaded in paragraphs 100 to 107 above;

(c) on 18 August 2022, by reason of the matters pleaded in paragraphs 100 to 109 above;

(d) on 15 September 2022, by reason of the matters pleaded in paragraphs 100 to 113 above.

**Particulars**

A. The representations were partly express and partly implied.

B. To the extent that they were express:

C. To the extent that they were express, the plaintiffs refer to:

1. as to (a), the plaintiffs refer to the matters in paragraph B to the particulars to paragraph 119 above together with the statement pleaded in paragraph 103 above, alternatively those matters read in the context of the matters pleaded in paragraphs 80 to 99 above;

2. as to (b), the plaintiffs refer to the matters in (i) above together with the statements pleaded in paragraphs 105 and 107 above, alternatively those matters read in the context of the matters pleaded in paragraphs 80 to 99 above;

3. as to (c), the plaintiffs refer to the matters in (ii) above together with the statement pleaded in 109 above, alternatively those matters read in the context of the matters pleaded in paragraphs 80 to 99 above;

4. as to (d), the plaintiffs refer to the matters in (iii) above together with the statements pleaded in paragraphs 111 and 113 above, alternatively those matters read in the context of the matters pleaded in paragraphs 80 to 99 above.

D. To the extent they were implied, they were implied by the statements referred to in B above and by the absence of Medibank making any statement that qualified or contradicted those statements.

121. Medibank represented to the Affected Market that (**Medibank's Cyber Security Representations**):

(a) it had IT Systems and processes that were effective at monitoring for and dealing with the Cyber Attack Risk; and

(b) there was no feature of Medibank's IT Systems and processes for collecting, storing and protecting its customers' personal and private information that made it likely that malicious cyber actors would be able to access and/or exfiltrate that information.

*D2.2 Medibank's Appropriate Access Representation*

122. Medibank represented to the Affected Market that Medibank's IT Systems and processes for collecting, storing and protecting its customers' personal and private information were such that only persons who required that data for the performance of their duties had access to that information (**Medibank's Appropriate Access Representation**).

*D2.3 Medibank's Standards Consistency Representation*

123. Medibank represented to the Affected Market that Medibank's cyber security framework was consistent with the standards, objects and outcomes described in industry standards and frameworks (**Medibank's Standards Consistency Representation**).

*D2.4 Medibank's Privacy Laws Compliance Representation*

124. Medibank represented to the Affected Market that Medibank's IT Systems and processes for collecting, storing and protecting its customers' personal and private information were sufficient to ensure compliance by Medibank with Australian Privacy Laws (**Medibank's Privacy Laws Compliance Representation**).

*D2.5 Continuing representations*

125. Medibank did not qualify or contradict Medibank's CPS 234 Compliance Representation, Medibank's Cyber Security Representations, Medibank's Appropriate Access Representation, Medibank's Standards Consistency Representation or Medibank's Privacy Laws Compliance Representation at any time from 5 September 2016 until the end of the Relevant Period after those representations were first made.

126. Each of Medibank's CPS 234 Compliance Representation, Medibank's Cyber Security Representations, Medibank's Appropriate Access Representation, Medibank's Standards Consistency Representation and Medibank's Privacy Laws Compliance Representation was a continuing representation throughout the Relevant Period.

## E. THE TRUE POSITION

127. At all times in the Relevant Period, Medibank's IT Systems and processes for collecting, storing and protecting the personal and private information of Medibank Customers and ahm

Customers had the following features (**Medibank's Cyber Safety Systems and Practices Deficiencies**):

(a) they did not involve sufficiently robust or effective at monitoring for, and identification of the use of, compromised credentials used to access Medibank's IT Systems;

(b) they were not sufficiently robust or effective to repel or prevent access to, and exfiltration of, the personal and private information of Medibank Customers and ahm Customers by malicious cyber actors;

(c) they did not have multi-factor authentication adequately deployed, such authentication comprising at least a username and password together with either:

(i) a digital certificate on the device used to access the IT Systems; or

(ii) another form of verification such as a code provided by email, SMS or phone application, or a hardware token;

(d) they were not appropriately configured in a way that required multi-factor authentication, or an additional digital security certificate, such that one single set of Medibank login credentials permitted access to Medibank's IT Systems and then the personal and private information of Medibank Customers and ahm Customers;

(e) they were not appropriately configured to prevent access to other Medibank credentials, which credentials permitted access to the personal and private information of Medibank Customers and ahm Customers;

(f) the personal and private information of Medibank Customers and ahm Customers held by Medibank was not, or not sufficiently, encrypted or anonymised to prevent it being read and understood once it was exfiltrated and disseminated; and

(g) by reason of the matters referred to in subparagraphs (a) to (f) above, Medibank's IT Systems and processes for collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers were not consistent with the Essential Cyber Security Requirements.

**Particulars**

A. As to (a), a criminal enterprise was able to use the stolen credentials to access Medibank's IT Systems and lurk there for an unknown period of time performing reconnaissance. Medibank only detected activity consistent with the precursor to a ransomware event: AFR, "Revealed: how

crooks got inside Medibank", 24 October 2022; Medibank announcement, "Medibank cyber incident and trading update", 17 October 2022. So far as the plaintiffs are able to say prior to discovery, media reporting is that the criminal enterprise "appear[s] to have had unfettered access to the insurer's data for at least several weeks": AFR, "Crims had free access to Medibank data, leaked emails show", 9 November 2022. The plaintiffs also refer to a statement by Koczkar that Medibank had no idea any customer data had been stolen until it was sent to the insurer: AFR, "Cocaine and opioids: Medibank hackers post stolen data", 9 November 2022.

B. As to (b), on 26 October 2022, Medibank announced that its investigation had established that a criminal enterprise had access to all Medibank, ahm and international students' personal data and significant amounts of health claims data. This amounted to as much as 200 gigabytes of data from Medibank servers including the location of where a customer received medical services and codes relating to their diagnosis and procedures: Australian Financial Review, "Privacy fallout from Medibank hack 'will be widespread'", 24 October 2022. Between 9 November 2022 and 1 December 2022, personal data and claims health data was released by the criminal enterprise.

C. As to (a), (c) and (d), so far as the plaintiffs can say prior to discovery, the plaintiffs refer to Medibank's HY23 Results "Investor Presentation" which states that "[t]he criminal accessed our systems using a stolen Medibank username and password used by a third party IT service provider … [t]he criminal used the stolen credentials to access Medibank's network through a misconfigured firewall which did not require an additional digital security certificate… The criminal was able to obtain further usernames and passwords to gain access to a number of Medibank's systems and their access was not contained": (p 7).

D. As to (e), so far as the plaintiffs can say prior to discovery, the plaintiffs refer to the fact of the dissemination of the information accessed and exfiltrated from Medibank in readable form by the malicious cyber actor or actors being the names, dates of birth, phone numbers and/or email addresses of around 9.7 million former and current customers, the names and locations of services providers from whom current and former Medibank Customers and ahm Customers received medical services, the codes associated with or identifying diagnoses made, and procedures administrated and treatment provider details.

E. As to (f), on or about 9, 10 and 14 November and 1 December 2022, a malicious cyber actor published data on the dark web which it had extracted from Medibank. Paragraphs A to D above and the particulars subjoined to paragraphs 65 and 66 above are repeated.

F. Further particulars may be provided following discovery and the filing of expert evidence.

128. At all times in the Relevant Period, by reason of Medibank's Cyber Safety Systems and Practices Deficiencies, Medibank's IT Systems and processes for collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers were not commensurate with (**Medibank's Information Security Controls Deficiencies**):

(a) the Cyber Attack Risk as pleaded in paragraph 27 above; and/or

(b) the seriousness of the consequences for Medibank Customers and ahm Customers of an information security incident, breach or threat involving unauthorised access, exfiltration, and/or dissemination of their personal and private information

**Particulars**

A. The plaintiffs refer to and repeats the: particulars subjoined to paragraphs 25, 26, 27, 28, 65, 66 and 127 above; the criticality and sensitivity of the information held by Medibank during the course of its business; and the existence of the Cyber Attack Risk and the Cyber Attack Risk Customer Consequences.

B. Further particulars may be provided following discovery and the filing of expert evidence.

129. At all times in the Relevant Period, by reason of Medibank's Cyber Safety Systems and Practices Deficiencies and Medibank's Information Security Controls Deficiencies, it was likely there would be, alternatively there was a material risk of, unauthorised access to, and the removal and distribution of, the personal and private information of a substantial number of Medibank Customers and ahm Customers by a malicious cyber actor (**Cyber Attack Vulnerability**).

**Particulars**

The Cyber Attack Vulnerability arose from Medibank's Cyber Safety Systems and Practices Deficiencies, Medibank's Information Security Controls Deficiencies and the matters pleaded in paragraph 130 below.

130. At all times in the Relevant Period, by reason of by reason of Medibank's Cyber Safety Systems and Practices Deficiencies, Medibank's Information Security Controls Deficiencies and the Cyber Attack Vulnerability, Medibank's IT Systems and processes for collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers had features that were not consistent with the standards, objects and outcomes described in industry standards and frameworks (**Medibank's Standards Deficiencies**).

**Particulars**

A. The plaintiffs refer to and repeat: the particulars subjoined to paragraphs 25 to 28, 37 to 64, 65, 66 and 127 to 129 above; the criticality and sensitivity of the information held by Medibank during the course of its business and the existence of the Cyber Attack Risk.

B. Further particulars may be provided following discovery and the filing of expert evidence.

131. At all times in the Relevant Period, by reason of Medibank's Information Security Controls Deficiencies, Medibank's IT Systems and processes for collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers had features that were not consistent with protecting personal information under Australian Privacy Laws (**Medibank's Privacy Laws Deficiencies**).

**Particulars**

A. The plaintiffs refers to and repeat: the particulars subjoined to paragraphs 25 to 28, 30 to 35, 65, 66 and 127 to 129 above; the criticality and sensitivity of the information held by Medibank during the course of its business; and the existence of the Cyber Attack Risk.

B. Further particulars may be provided following discovery and the filing of expert evidence.

## F. MISLEADING OR DECEPTIVE CONDUCT

132. The making of each of Medibank's CPS 234 Compliance Representation, Medibank's Cyber Security Representations, Medibank's Appropriate Access Representation, Medibank's Standards Consistency Representation and Medibank's Privacy Laws Compliance Representation was conduct engaged in by Medibank:

(a) in relation to financial products (being MPL Shares), within the meaning of s 1041H(1) of the *Corporations Act*;

(b) in trade or commerce in relation to financial services within the meaning of s 12DA of the ASIC Act; and/or

(c) in trade or commerce, within the meaning of s 18 of the ACL.

### F1. Medibank's CPS 234 Compliance Representation

133. By reason of the matters pleaded in paragraph 148 below, from 10 September 2020 to the end of the Relevant Period, in making, maintaining and/or failing to correct or qualify Medibank's

CPS 234 Compliance Representation, Medibank engaged in conduct which was misleading or deceptive, or likely to mislead or deceive.

134. By reason of the matters pleaded in paragraphs 132 and 133 above, from 10 September 2020 to the end of the Relevant Period, Medibank contravened s 1041H of the *Corporations Act*, s 12DA(1) of the ASIC Act and/or s 18 of the ACL (**Medibank's CPS 234 Misleading Conduct Contravention**).

**F2. Medibank's Cyber Security Representations Contravention**

135. By reason of the matters pleaded in paragraphs 127 to 131 above, from 10 September 2020 to the end of the Relevant Period, alternatively from the date in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, in making, maintaining and/or failing to correct or qualify Medibank's Cyber Security Representations, Medibank engaged in conduct which was misleading or deceptive, or likely to mislead or deceive.

136. By reason of the matters pleaded in paragraphs 132 and 135 above, on and from 10 September 2020, alternatively from the date in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, Medibank contravened s 1041H of the Corporations Act, s 12DA(1) of the ASIC Act and/or s 18 of the ACL (**Medibank's Cyber Security Misleading Conduct Contravention**).

**F3. Medibank's Appropriate Access Representation Contravention**

137. By reason of the matters pleaded in paragraphs 127 to 131 above, from 10 September 2020 to the end of the Relevant Period, alternatively from the date in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, in making, maintaining and/or failing to correct or qualify Medibank's Appropriate Access Representation, Medibank engaged in conduct which was misleading or deceptive, or likely to mislead or deceive.

138. By reason of the matters pleaded in paragraphs 132 and 137 above, on and from 10 September 2020, alternatively from the date in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, Medibank contravened s 1041H of the Corporations Act, s 12DA(1) of the ASIC Act and/or s 18 of the ACL (**Medibank's Appropriate Access Misleading Conduct Contravention**).

**F4. Medibank's Standards Consistency Representation Contravention**

139. By reason of the matters pleaded in paragraphs 127 to 131 above, from 10 September 2020 to the end of the Relevant Period, alternatively from the dates in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, in making, maintaining and/or

failing to correct or qualify Medibank's Standards Consistency Representation, Medibank engaged in conduct which was misleading or deceptive, or likely to mislead or deceive.

140. By reason of the matters pleaded in paragraphs 132 and 139 above, on and from 10 September 2020, alternatively from the dates in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, Medibank contravened s 1041H of the Corporations Act, s 12DA(1) of the ASIC Act and/or s 18 of the ACL (**Medibank's Standards Consistency Misleading Conduct Contravention**).

### F5. Medibank's Privacy Laws Compliance Representation Contravention

141. By reason of the matters pleaded in paragraphs 127 to 131 above, from 10 September 2020 to the end of the Relevant Period, alternatively from the dates in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, on and from 10 September 2020, in making, maintaining and/or failing to correct or qualify Medibank's Privacy Laws Compliance Representation, Medibank engaged in conduct which was misleading or deceptive, or likely to mislead or deceive.

142. By reason of the matters pleaded in paragraphs 132 and 141 above, on and from 10 September 2020, alternatively from the dates in subparagraph (a), (b), (c) or (d) of paragraph 120 above to the end of the Relevant Period, Medibank contravened s 1041H of the Corporations Act, s 12DA(1) of the ASIC Act and/or s 18 of the ACL (**Medibank's Privacy Laws Compliance Misleading Conduct Contravention**).

## G. CONTINUOUS DISCLOSURE CONTRAVENTIONS

### G1. MFA Information

143. At all times in the Relevant Period, Medibank did not have in place multifactor authentication for all persons with access to its network (**MFA Information**).

**Particulars**

As pleaded above, malicious cyber actors were able to access Medibank's network without multifactor authentication.

### G2. Lack of Network Control System Information

144. At all times in the Relevant Period, Medibank did not have in place a network control system comprising all of the following (**Lack of Network Control System Information**):

(a) a system for monitoring unusual activity in respect of Medibank's network;

(b) an endpoint detection and response system to identify the presence of malicious software on Medibank's network;

(c) a system for monitoring for "lateral movement" within Medibank's network (that is, movement between different systems within Medibank's network); and

(d) a system for preventing the extraction of substantial volumes of data from Medibank's network.

**Particulars**

As pleaded above, malicious cyber actors were able to access Medibank's network and extract substantial volumes of data. It is to be inferred from this that one or more of the components of a network control system pleaded above was absent.

**G3. The Cyber Security Failure and Compliance Deficiencies Information**

145. At all times in the Relevant Period, by reason of Medibank's Cyber Safety Systems and Practices Deficiencies, Medibank's Information Security Controls Deficiencies, the Cyber Attack Vulnerability, Medibank's Standards Deficiencies and/or Medibank's Privacy Laws Deficiencies (collectively, the **Cyber Deficiencies**):

(a) Medibank's IT Systems and processes for collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers were ineffective to prevent that data being accessed, removed, and disseminated in readable form by hackers; and/or

(b) Medibank's IT Systems and processes in respect of cyber security and privacy protection were ineffective to manage the risk that Medibank's systems for collecting, storing and accessing personal and private information of Medibank Customers and ahm Customers would be a target for cyber-related attacks and cybercrime

(**Cyber Security Failure and Compliance Deficiencies Information**).

**G4. The Cyber Security Standards Non-Compliance Information**

146. At all times in the Relevant Period, by reason of the Cyber Deficiencies:

(a) Medibank's IT Systems and processes in relation to collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers were not consistent with industry standards and frameworks applicable to the

protection of personal and private information of the kind collected by Medibank; and/or

(b) Medibank's IT Systems and processes in relation to collecting, storing and protecting the personal and private information of Medibank Customers and ahm Customers were not consistent with protecting personal information under Australian Privacy Laws

(**Cyber Security Standards Non-Compliance Information**).

**G5. The Cyber Attack Vulnerability Information**

147. At all times in the Relevant Period, by reason of the Cyber Deficiencies, it was likely there would be, alternatively there was a material risk of, unauthorised access to, and the removal and distribution of, the personal and private information of a substantial number of Medibank Customers and ahm Customers by a hacker (**Cyber Attack Vulnerability Information**).

**G6. Breach of CPS 234 Information**

148. By reason of each of the matters pleaded in 143 to 147 above, alternatively any combination of those matters, from 1 July 2019 to the end of the Relevant Period, Medibank was in breach of paragraphs 15, 21 and 23 of CPS 234 (**Breach of CPS 234 Information**).

**G7. Contravention of s 674(2) of the *Corporations Act***

149. At all times in Relevant Period, Medibank was:

(a) as pleaded above, a "listed disclosing entity" for the purposes of s 674 of the *Corporations Act*;

(b) bound by the provisions of the ASX Listing Rules, including those that required an entity to notify the ASX of information about specified events or matters as they arose for the purpose of the ASX making that information available to participants in the market; and

(c) in the premises, pursuant to s 674(1) of the *Corporations Act*, an entity to which s 674(2) of the *Corporations Act* applied (within the meaning of s 674(2)(a) of the *Corporations Act*).

150. By at least the beginning of the Relevant Period, an officer of Medibank ought reasonably to have come into possession, in the course of the performance of his or her duties as an officer of Medibank, of:

(a) the MFA Information;

(b) the Lack of Network Control System Information;

(c) the Cyber Security Failure and Compliance Deficiencies Information;

(d) the Cyber Security Standards Non-Compliance Information

(e) the Cyber Attack Vulnerability Information; and/or

(f) the Breach of CPS 234 Information

(individually or collectively, the **Material Information**).

**Particulars**

A. As to the officers of Medibank as at the beginning of the Relevant Period, the plaintiffs refer to paragraphs 7, 9, 10, 11, 12, 16, 17, 18, 19, 20, 21 and 23 above.

B. Medibank was obliged to comply with CPS 234. A draft of CPS 234 was released in March 2018. The final was made in November 2018, approximately seven months before it commenced operation on 1 July 2019. In these circumstances, and having regard to the requirements of CPS 234 pleaded above, it is to be inferred that the Material Information existed within Medibank by at least 1 July 2019. In light of the ultimate responsibility imposed on the Board by CPS 234, and in light of the requirements under CPS 234 concerning escalation of information security control deficiencies to the Board and senior management, the Material Information ought reasonably to have come into possession of an officer of Medibank.

151. By reason of the matters pleaded in paragraph 150 above, by at least the beginning of the Relevant Period, Medibank was aware of the Material Information within the meaning of listing rule 3.1 of the ASX Listing Rules.

152. At all times in the Relevant Period, the Material Information was information concerning Medibank that a reasonable person would expect to have a material effect on the price or value of MPL Shares within the meaning of listing rule 3.1 of the ASX Listing Rules.

153. At all times in the Relevant Period, by reason of the matters pleaded in paragraphs 151 and 152 above, Medibank had information that listing rule 3.1 of the ASX Listing Rules required Medibank to notify to the ASX (namely, the Material Information) within the meaning of s 674(2)(b) of the *Corporations Act*.

154. At all times in the Relevant Period, the Material Information was not generally available within the meaning of s 674(2)(c) of the *Corporations Act*.

**Particulars**

The plaintiffs refer to s 676 of the *Corporations Act* as in force during the Relevant Period, which addressed when information was generally available.

155. At all times in the Relevant Period, the Material Information was information that a reasonable person would expect, if it were generally available, to have a material effect on the price or value of MPL Shares, within the meaning of s 674(2)(c)(ii) of the *Corporations Act* and s 674(2)(d) of the *Corporations Act*.

**Particulars**

The plaintiffs refer to s 677 of the *Corporations Act* as in force during the Relevant Period, which addressed when a reasonable person would be taken to expect information to have a material effect on the price or value of securities.

As to the reference above to both s 674(2)(c)(ii) and s 674(2)(d), on 14 August 2021, s 674(2) was amended so that the materiality requirement previously found in s 674(2)(c)(ii) was relocated to new s 674(2)(d): see *Treasury Laws Amendment (2021 Measures No. 1) Act 2021*, Schedule 2, item 3.

156. Further, in the period 26 May 2020 to 23 March 2021, Medibank:

(a) ought to have known that the Material Information would, if it were generally available, have a material effect on the price or value of MPL Shares; and

(b) in the premises, was negligent with respect to whether the Material Information would, if it were generally available, have a material effect on the price or value of MPL Shares, within the meaning of s 674(2)(d) of the *Corporations Act*.

**Particulars**

The plaintiffs refer to the *Corporations (Coronavirus Economic Response) Determination (No. 2) 2020* and *Corporations (Coronavirus Economic Response) Determination (No. 4) 2020* and to s 677 of the *Corporations Act* as it stood while those instruments were in force.

Prior to the two determinations to which reference has been made, s 674(2)(c) provided as follows: "that information: (i) is not generally available; and (ii) is information that a reasonable person would expect, if it were generally available, to have a material effect on the price or value of ED securities of the entity". The two determinations to which reference has been made temporarily omitted section 674(2)(c) and replaced it with the following: "(c) that information is not generally available; and (d) the entity knows or is reckless or negligent with respect to whether that information would, if it were generally available, have a material effect on the price or value of ED securities of the entity". A consequential modification was also made

to s 677 by the instruments referred to. These temporary changes expired on 23 March 2021. They were effectively reinstated, on a permanent basis, on 14 August 2021, by the introduction of s 674A (see paragraphs 160 to 168 below).

157. By reason of the matters pleaded at paragraphs 149 to 156 above, on and from 1 July 2019 to the end of the Relevant Period, Medibank was obliged by s 674(2) of the *Corporations Act* to notify the ASX of the Material Information.

158. Medibank did not notify the ASX of the Material Information during the Relevant Period.

159. By reason of the matters pleaded at paragraphs 157 to 158 above, on and from 1 July 2019 until the end of the Relevant Period, Medibank contravened s 674(2) of the *Corporations Act.*

**Contravention of section 674A(2) of the *Corporations Act***

160. On 14 August 2021, s 674A of the *Corporations Act* commenced operation.

**Particulars**

The plaintiffs refer to the *Treasury Laws Amendment (2021 Measures No. 1) Act 2021*, s 2, item 3 of the table therein.

161. From 14 August 2021 to the end of the Relevant Period, Medibank was:

(a) as pleaded above, a "listed disclosing entity" for the purposes of s 674A of the *Corporations Act*; and

(b) by reason of the matters pleaded in subparagraph (a) above and paragraph 149(b) above, an entity to which s 674A(2) of the *Corporations Act* applied (within the meaning of s 674A(2)(a) of the *Corporations Act*).

162. Paragraphs 150 to 152 above are repeated.

163. From 14 August 2021 to the end of the Relevant Period, by reason of the matters pleaded in paragraph 162 above, , Medibank had information that listing rule 3.1 of the ASX Listing Rules required Medibank to notify to the ASX (namely, the Material Information) within the meaning of s 674A(2)(b) of the *Corporations Act*.

164. From 14 August 2021 to the end of the Relevant Period, the Material Information was not generally available within the meaning of s 674A(2)(c) of the *Corporations Act*.

**Particulars**

The plaintiffs refer to s 676 of the *Corporations Act* as in force during the Relevant Period.

165. From 14 August 2021 to the end of the Relevant Period, Medibank:

(a) ought to have known that the Material Information would, if it were generally available, have a material effect on the price or value of MPL Shares; and

(b) in the premises, was negligent with respect to whether the Material Information would, if it were generally available, have a material effect on the price or value of MPL Shares, within the meaning of s 674A(2)(d) of the *Corporations Act*.

166. By reason of the matters pleaded at paragraphs 160 to 165 above, on and from 14 August 2021 to the end of the Relevant Period, Medibank was obliged by s 674A(2) of the *Corporations Act* to notify the ASX of the Material Information.

167. Paragraph 158 above is repeated.

168. By reason of the matters pleaded at paragraphs 166 to 167 above, on and from 14 August 2021 until the end of the Relevant Period, Medibank contravened s 674A(2) of the *Corporations Act*.

## H. RELEVANT ANNOUNCEMENTS BY MEDIBANK, TRADING HALTS AND CHANGES IN THE SHARE PRICE

### H1. Announcements and trading halts

169. On 13 October 2022:

(a) the trading of MPL Shares on the ASX was temporarily paused pending a further announcement;

(b) the trading of MPL Shares on the ASX was subsequently halted (**First Trading Halt**); and

(c) Medibank published an announcement to the ASX entitled "Medibank Cyber Incident" (**13 October Announcement**).

170. The last price at which MPL Shares traded prior to the First Trading Halt was $3.52.

**Particulars**

$3.52 was the price at which MPL Shares closed on 12 October 2022. A temporary pause in trading was announced at 9.59 am on 13 October 2022, just before the market opened. The First Trading Halt was then announced at 11.27 am on the same day. The 13 October Announcement was released simultaneously with that announcement.

171. In the 13 October Announcement, Medibank made the following statements:

(a) "Yesterday the Medibank Group detected unusual activity on its network. In response to this event, Medibank took immediate steps to contain the incident, and engaged specialised cyber security firms. At this stage there is no evidence that any sensitive data, including customer data, has been accessed. As part of our response to this incident, Medibank will be isolating and removing access to some customer-facing systems to reduce the likelihood of damage to systems or data loss."

(b) "As a result our ahm and international student policy management systems have been taken offline. We expect these systems to be offline for most of the day. This will cause regrettable disruptions for some of our customers. ahm and international student customers will still be able to contact our customer teams via phone but at this stage our people won't be able to access policy information."

(c) "As we continue to investigate this incident, our priorities are to ensure the ongoing security of customers, our employees, and stakeholder information, and the continued delivery of Medibank services. Investigations are ongoing, and Medibank will provide regular updates. Medibank's health services continue to be available to our customers, this includes their ability to access their health providers, as we work through this incident."

172. On 17 October 2022:

(a) Medibank published an announcement to the ASX entitled "Medibank cyber incident and trading update" (**17 October Announcement**);

(b) trading of MPL Shares on the ASX resumed; and

(c) MPL Shares closed at $3.40.

173. In the 17 October Announcement, Medibank made the following statements:

(a) "The Medibank Group today confirmed that ongoing investigations continue to show there remains no evidence customer data has been removed from its IT environment, after it detected unusual activity last week in part of its IT network."

(b) "Normal operations have resumed, and Medibank will continue to investigate the incident as part of its ongoing forensic analysis. When the unusual activity was detected on part of its network, the company took the precautionary action to temporarily block and isolate access to the ahm and international student customer

policy management systems while the activity was investigated. This was done out of an abundance of caution, and it enabled Medibank to provide additional protection of customer data on that system. The systems were restored on new IT infrastructure and normal activity resumed for ahm and international student business on Friday 14 October 2022."

(c) "Medibank also deployed additional security measures across its network, strengthening the integrity of its systems. Medibank has contained the ransomware threat but remains vigilant and will take necessary steps in the future to protect its operations and its customers' data."

(d) "Medibank's investigation, which is ongoing, indicated that its cyber security systems had detected activity consistent with the precursor to a ransomware event. This initial finding was shared with the Australian Cyber Security Centre, who provided Medibank with additional guidance in support of this conclusion. Medibank systems were not encrypted by ransomware during this incident and there is no indication that the incident was caused by a state-based threat actor."

(e) "As a health company providing health insurance and health services, Medibank holds a range of necessary personal information of customers, and the protection of customers' data security is its highest priority. Medibank is continuing to work with external parties to provide them with assurance about this incident, and Medibank's recovery. During this incident customers have continued to be able to access health services and their health providers during this time."

(f) "The Australian Cyber Security Centre (the Australian Government lead agency) was engaged and Medibank is working in an open and cooperative manner with them to both keep national response agencies updated and to receive information and intelligence which is assisting with the resolution of the incident."

174. On 18 October 2022, MPL Shares closed at $3.50.

175. On 19 October 2022:

(a) the trading of MPL Shares on the ASX was temporarily paused pending a further announcement;

(b) the trading of MPL Shares on the ASX was subsequently halted (**Second Trading Halt**); and

(c) Medibank published an announcement to the ASX entitled "Medibank cyber incident update" (**19 October Announcement**).

**Particulars**

The temporary pause in trading was announced at 11.53 am. The Second Trading Halt was announced at 12.48 pm. The 19 October Announcement was released at 4.45 pm.

176. The price at which MPL Shares were trading immediately prior to the Second Trading Halt was $3.505.

177. In the 19 October Announcement, Medibank made the following statements:

(a) "Today Medibank Group has received messages from a group that wishes to negotiate with the company regarding their alleged removal of customer data. This is a new development and Medibank understands this news will cause concerns for customers and the protection of their data remains our priority."

(b) "Medibank is working urgently to establish if the claim is true, although based on our ongoing forensic investigation we are treating the matter seriously at this time."

(c) "As a health company providing health insurance and health services, Medibank holds a range of necessary personal information of customers. Medibank systems have not been encrypted by ransomware, which means usual activities for customers continues. Medibank will continue to keep our customers updated."

(d) "As a result of this, Medibank has entered into a trading halt, to ensure that it meets its continuous disclosure obligations. The trading halt will continue until further notice. We continue to work with specialised cyber security firms and have advised the Australian Cyber Security Centre (ACSC). Our ongoing response to safeguard our networks and systems may cause necessary temporary disruptions to our services."

178. On 20 October 2022, Medibank published an announcement to the ASX entitled "Medibank cyber incident response" (**20 October Announcement**).

179. In the 20 October Announcement, Medibank made the following statements:

(a) "This cyber incident is now the subject of an investigation by the Australian Federal Police. We know that our customers, people, and the community want to know what data has been stolen, and how that may affect them."

(b) "Here is what we can currently share. Medibank has been contacted by a criminal claiming to have stolen 200GB of data. The criminal has provided a sample of records for 100 policies which we believe has come from our ahm and international student systems. That data includes first names and surnames, addresses, dates of birth, Medicare numbers, policy numbers, phone numbers and some claims data. This claims data includes the location of where a customer received medical services, and codes relating to their diagnosis and procedures. The criminal claims to have stolen other information, including data related to credit card security, which has not yet been verified by our investigations."

(c) "What we are doing now. Medibank teams continue to work around the clock to understand what additional customer data has been affected, and how this will impact them. This morning we will commence making direct contact with the affected customers to inform them of this latest development, and to provide support and guidance on what to do next. We expect the number of affected customers to grow as the incident continues. We will continue to contact affected customers."

180. On 21 October 2022, MPL Shares were suspended from quotation on the ASX.

181. On 25 October 2022, Medibank published an announcement to the ASX entitled "Medibank cybercrime update" (**25 October Announcement**).

182. In the 25 October Announcement, Medibank made the following statements:

(a) "There has been a further development in Medibank's cybercrime event, which is subject to a criminal investigation by the Australia Federal Police (AFP). It has become clear that the criminal has taken data that now includes Medibank customer data, in addition to that of ahm and international student customers. This is a distressing development and Medibank unreservedly apologises to our customers."

(b) "Here is what we can update. We have received a series of additional files from the criminal. We have been able to determine that this includes: • A copy of the file received last week containing 100 ahm policy records – including personal and health claims data • A file of a further 1,000 ahm policy records – including personal and health claims data • Files which contain some Medibank and additional ahm and international student customer data."

(c) "Given the complexity of what we have received, it is too soon to determine the full extent of the customer data that has been stolen. We will continue to analyse what we

have received to understand the total number of customers impacted, and specifically which information has been stolen. We have taken the step of making this announcement as we believe it is important to notify our customers of this development. As we continue to investigate the scale of this cybercrime, we expect the number of affected customers to grow as this unfolds."

183. On 26 October 2022:

(a) Medibank published an announcement to the ASX entitled "Medibank cybercrime, business and FY23 update" (**26 October Announcement**);

(b) MPL Shares were reinstated to quotation; and

(c) MPL Shares closed at $2.87, which represented an 18.117% drop from the price of $3.505 at which they were trading immediately prior to the commencement of the Second Trading Halt (see paragraph 176 above).

**Particulars**

The 26 October Announcement and the reinstatement to quotation were announced simultaneously, at 9.32 am.

184. In the 26 October Announcement, Medibank made the following statements:

(a) "Yesterday, Medibank provided a further update regarding the cybercrime event and announced a comprehensive customer support package for Medibank, ahm and international student customers affected by this cybercrime."

(b) "The investigation into the cybercrime event is continuing, with particular focus on identifying which systems and networks were accessed and what data was removed by the criminal. Since yesterday's announcement, our investigation has now established that the criminal had access to: • All ahm customers' personal data and significant amounts of health claims data • All international student customers' personal data and significant amounts of health claims data • All Medibank customers' personal data and significant amounts of health claims data".

(c) As previously advised, we have evidence that the criminal has removed some of our customers' personal and health claims data and it is now likely that the criminal has stolen further personal and health claims data. As a result, we expect that the number of affected customers could grow substantially."

(d) "To date, Medibank's IT systems have not been encrypted by ransomware. Normal business operations have been maintained with customers continuing to access health services."

(e) "Concurrent to the investigation, Medibank has prioritised preventing further unauthorised entry to our IT network and is continuing to monitor for any further suspicious activity. This has included bolstering existing monitoring, adding further detection and forensics capability across Medibank's systems and network and scaling up analytical support via specialist third parties."

(f) "This cybercrime event is subject to a criminal investigation by the Australian Federal Police (AFP). Medibank continues to work with the AFP, specialised cyber security firms, the Australian Cyber Security Centre (ACSC) and government stakeholders."

(g) "Given the uncertain impact of this cybercrime event, Medibank is withdrawing its FY23 outlook for policyholder growth and will provide a further update at the 1H23 results."

(h) "Based on our current actions in response to the cybercrime event, noting that Medibank does not have cyber insurance, we currently estimate $25 million-$35 million pre-tax non-recurring costs will impact earnings in 1H23. These non-recurring costs do not include further potential customer and other remediation, regulatory or litigation related costs. This cybercrime event continues to evolve and at this stage, we are unable to predict with any certainty the impact of any future events on Medibank including the quantum of any potential customer and other remediation, regulatory or litigation related costs."

(i) (attributed to Koczkar) "Our investigation has now established that this criminal has accessed all our private health insurance customers personal data and significant amounts of their health claims data."

(j) (attributed to Koczkar) "As we've continued to say we believe that the scale of stolen customer data will be greater and we expect that the number of affected customers could grow substantially."

**H2. Impact of the announcements**

185. Following the release of the announcements pleaded in paragraphs 177, 179, 182 and 184 above (**Access and Removal Disclosures**):

(a) the price of MPL Shares fell materially; and

(b) the value of MPL Equity Swaps was materially adversely affected.

**Particulars**

A. The price of MPL Shares dropped by 18% from the price of $3.505 at which they were trading immediately prior to the commencement of the Second Trading Halt.

B. Further particulars may be provided following the filing of expert evidence.

## I. CONTRAVENING CONDUCT CAUSED LOSS

### I1. Market-based causation

*I1.1 MPL Shares*

186. The plaintiffs and some Group Members acquired an interest in MPL Shares in a market of investors or potential investors in MPL Shares in circumstances where:

(a) Medibank was obliged by s 674(2) and/or s 674A(2) of the *Corporations Act* to notify information of the kind referred to in those provisions to the ASX so that the information could be disclosed to the market;

(b) the price of MPL Shares was affected by information notified to the ASX in accordance with that obligation;

(c) the price of MPL Shares was affected by representations made by Medibank to the market;

(d) Medibank was obliged by s 1041H of the *Corporations Act* and/or s 12DA of the ASIC Act and/or s 18 of the ACL not to make representations to the market that were misleading or deceptive or likely to mislead or deceive.

187. By reason of the contraventions pleaded in paragraphs 159 and 168 above (**Continuous Disclosure Contraventions**), and/or the contraventions pleaded in paragraphs 134, 136, 138, 140 and 142 above (**Misleading Conduct Contraventions**), the information available to the market of investors and potential investors in MPL Shares was different from the information that would have been available to that market had those contraventions not occurred.

188. During the Relevant Period, the Continuous Disclosure Contraventions and/or the Misleading Conduct Contraventions caused the price of MPL Shares in the Affected Market to be, or materially contributed to the price of MPL Shares in that market being, substantially greater than:

(a) the true value of MPL Shares; and/or

(b) the price of MPL Shares that would have prevailed but for the Continuous Disclosure Contraventions and/or the Misleading Conduct Contraventions.

**Particulars**

Particulars of the extent to which the contraventions caused the price of MPL Shares to be, or materially contributed to the price of MPL Shares being, greater than their true value and/or greater than the price that would otherwise have prevailed during the Relevant Period will be provided by way of the plaintiffs' expert evidence.

189. The material fall in the price of MPL Shares pleaded in paragraph 185(a) above was caused or materially contributed to by:

(a) the market's reaction to the Access and Removal Disclosures; and

(b) by reason of the matters pleaded in paragraphs 186 to 188 above, the Continuous Disclosure Contraventions and/or the Misleading Conduct Contraventions.

*I1.2 MPL Equity Swaps*

190. At all times in the Relevant Period, the market for MPL Equity Swaps was a market that traded on the basis that the market for MPL Shares had the features pleaded in paragraph 186 above.

191. By reason of the matters pleaded in paragraphs 186 to 190 above, when during the Relevant Period Group Members who entered into MPL Equity Swaps entered into those swaps, did so at a time when:

(a) the market price for MPL Shares was substantially greater than;

(i) the true value of MPL Shares; and/or

(ii) the price of MPL Shares that would have prevailed but for the Continuous Disclosure Contraventions and/or the Misleading Conduct Contravention;

(b) the MPL Equity Swaps had been defined by reference to the market price of MPL Shares in circumstances where that maker price was as set out in (a) above; and

(c) by reason of the matters in (a) and (b) above, the value of the future cashflows to be received by the equity amount receiver pursuant to the MPL Equity Swaps by reference to the performance of MPL Shares was diminished and/or the value of the cashflows to be paid by the equity amount receiver in return was inflated.

## I2. Reliance

192. Further, or in the alternative to paragraphs 186 to 189 above in deciding to acquire an interest in MPL Shares:

(a) the plaintiffs and some Group Members would not have entered into the transactions pursuant to which they acquired an interest in MPL Shares if they had known the Material Information; and/or

(b) some Group Members relied directly on some or all of:

(i) the representations the subject of the Misleading Conduct Contraventions; and/or

(ii) the absence of any correction of or qualification to those representations.

**Particulars**

A. The plaintiffs would not have entered into the transactions pursuant to which they acquired an interest in MPL Shares had they known of the Material Information.

B. The identities of all those Group Members who would not have entered into the transactions pursuant to which they acquired an interest in MPL Shares had they known of any or all of the Material Information, and/or who relied on any or all of the representations the subject of the Misleading Conduct Contraventions, are not presently known to the plaintiffs and cannot be ascertained unless and until those advising the plaintiffs take detailed instructions from all Group Members on individual issues relevant to the determination of those individual Group Members' claims. Those instructions will be obtained (and particulars of the identity of those Group Members will be provided) following opt out, the determination of the plaintiffs' claims and identified common issues at an initial trial and if and when it is necessary for a determination to be made of the individual claims of those Group Members.

193. Further, or in the alternative to paragraphs 190 to 191 above, in deciding to acquire MPL Equity Swaps some Group Members:

(a) would not have acquired MPL Equity Swaps by reference to the price for, and volume of, MPL Shares that they did, if they had known of the Material Information; and/or

(b) acquired MPL Equity Swaps by reference to a price of MPL Shares in reliance upon some or all of:

(i) the representations the subject of the Misleading Conduct Contraventions; and/or

(ii) the absence of any correction of or qualification to the representations the subject of those contraventions.

**I3. Loss or damage suffered by the plaintiffs and Group Members**

194. By reason of the matters pleaded in paragraphs 186 to 193 above, the plaintiffs and Group Members have suffered loss or damage by, because of and/or resulting from the Continuous Disclosure Contraventions and/or the Misleading Conduct Contraventions.

**Particulars**

A. The measure of each plaintiff's loss will be the greater of:

a. the difference between the price at which he acquired the MPL Shares during the Relevant Period and the price that would have prevailed but for the Continuous Disclosure Contraventions and/or the Misleading Conduct Contraventions (the "inflation-based measure");

b. the difference between the price at which he acquired MPL Shares during the Relevant Period and the true value of those shares (the "true value measure");

c. the difference between the price at which he acquired MPL Shares during the Relevant Period and whatever is "left in hand" upon a sale (the "left in hand measure");

d. the difference between the position he is in at the date of the trial as a result of acquiring MPL shares during the Relevant Period and the position he would have been in had he not acquired those shares (the "no transaction measure");

B. Further particulars in relation to each plaintiff's losses will be provided after the service of evidence in chief.

C. Paragraph B of the particulars to paragraph 192 above is repeated.

**J. COMMON QUESTIONS OF LAW OR FACT**

195. The questions of law or fact common to the claims of the Group Members are as follows:

(a) whether the facts are as pleaded in paragraphs 2 to 4, 6 to 24, 25(a), 26 to 29, 31, 37 to 42, 65, 66, 68 to 79, 80,117, 125 to 131, 143 to 147, 158, 167, and 169 to 194 above;

(b) whether, during the Relevant Period, Medibank made and failed to correct:

(i) Medibank's CPS 234 Compliance Representation;

(ii) Medibank's Cyber Security Representations;

(iii) Medibank's Appropriate Access Representation;

(iv) Medibank's Standards Consistency Representation; and

(v) Medibank's Privacy Laws Representation;

(c) whether the matters in (b) constituted conduct in relation to financial products within the meaning of s 1041H(1) of the Corporations Act, in trade or commerce in relation to financial services within the meaning of s 12DA of the ASIC Act, and/or in trade or commerce within the meaning of s 18 of the ACL;

(d) whether, having regard to (a) and (c) above, Medibank committed the Misleading Conduct Contraventions;

(e) whether, during the Relevant Period, and for the purposes of listing rule 3.1 of the ASX Listing Rules:

(i) Medibank was aware of the Material Information; and

(ii) the Material Information was information that a reasonable person would expect to have a material effect on the price or value of Medibank Shares;

(f) whether, during the Relevant Period, and for the purposes of s 674(2) and s 674A(2) of the *Corporations Act*:

(i) Medibank had information that listing rule 3.1 of the ASX Listing Rules required Medibank to notify to the ASX, namely, the Material Information;

(ii) the Material Information was not generally available;

(iii) the Material Information was information that a reasonable person would expect, if it were generally available, to have a material effect on the price or value of Medibank Shares;

(iv) Medibank was negligent with respect to whether the Material Information would, if it were generally available, have a material effect on the price or value of Medibank Shares;

(v) whether, having regard to (d) to (e) above, Medibank committed the Continuous Disclosure Contraventions; and

(g) whether the plaintiffs and Group Members have suffered loss or damage by, because of or resulting from the Continuous Disclosure Contraventions and/or the Misleading Conduct Contraventions and are entitled to compensation for that loss or damage.

**AND THE PLAINTIFFS' CLAIM ON THEIR OWN BEHALF AND ON BEHALF OF GROUP MEMBERS:**

A. A declaration that Medibank engaged in conduct in contravention of:

(a) s 674 and s 674A of the *Corporations Act*;

(b) s 1041H(1) of the *Corporations Act*;

(c) s 12DA(1) of the ASIC Act;

(d) s 18 of the ACL.

B. An order pursuant to s 1317HA(1) of the *Corporations Act* that Medibank pay compensation to the plaintiffs and Group Members for loss or damage resulting from the conduct of Medibank in contravention of s 674(2) and s 674A(2) of the *Corporations Act*.

C. An order pursuant to s 1041I of the *Corporations Act* that Medibank pay compensation to the plaintiffs and Group Members for loss or damage caused by the conduct of Medibank in contravention of s 1041H of the *Corporations Act*.

D. An order pursuant to s 12GF of the ASIC Act that Medibank pay compensation to the plaintiffs and Group Members for loss or damage caused by the conduct of Medibank in contravention of s 12DA(1) of the ASIC Act.

E. An order pursuant to s 236 of the ACL that Medibank pay compensation to the plaintiffs and Group Members for loss or damage suffered because of the conduct of Medibank in contravention of s 18 of the ACL.

F. Interest pursuant to statute on any damages, compensation or other monetary sum awarded.

G. Costs.

Such further order as the Court determines is appropriate

**Dated**: 3 October 2023

……..

**Quinn Emanuel Urquhart & Sullivan**

**Phi Finney McDonald**

Joint solicitors for the plaintiffs

**THIS WRIT** is to be served within one year from the date it is filed or within such further period as the Court orders.

1. Place of trial — Melbourne
2. Mode of trial — Judge
3. This writ was filed for the plaintiffs by Quinn Emanuel Urquhart & Sullivan as joint solicitors for the plaintiffs.
4. The address of the first plaintiff is — [redacted]

   The address of the second plaintiff is — [redacted]
5. The address for service of the plaintiff is — c/o Phi Finney McDonald, Level 3, 325 Flinders Lane, Melbourne VIC 3000.
6. The email address for service of the plaintiffs is — medibankclassaction@phifinneymcdonald.com
7. The address of the defendant is — Level 6, 720 Bourke St, Docklands, VIC 3008