Annexure B – Steps to protect personal information held by Medibank

Having regard to its size, resources, the nature and volume of the personal information it held (which included sensitive information, such as information about its customers' race and ethnicity and health information), and the risk of harm for an individual in the case of a breach, during the Relevant Period it was reasonable for Medibank to adopt all, or alternatively some combination sufficient to its circumstances, of the following measures to protect the personal information it held:

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

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

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

4 Implement appropriate privileged access management controls by:

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

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

5 Implement appropriate monitoring for privileged accounts, including by:

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

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

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

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

(a) undertaking regular password usage audits; and

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

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

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

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

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

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

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

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

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

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

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

11 Implement effective contractor assurance, including by:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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