Allens

In alliance with Linklaters

Comparative analysis of suggested cybersecurity measures

This table provides a comparative analysis of security measures class action plaintiffs and regulators have alleged are required in proceedings following significant cyber security failures. It considers two consumer class actions, one shareholder class action and two regulatory proceedings, one by ASIC and the other by the OAIC.

Note: Three other proceedings have not been included in the table below as limited information is available as to the security measures alleged to be required. These include ASIC's proceedings against Fortnum Private Wealth, OAIC's proceedings against Australian Clinical Labs, and ASIC's finalised proceedings against RI Advice.

	Medibank Consolidated Consumer Claim (Baker McKenzie)	Optus Consumer Claim (Slater & Gordon)	Medibank Consolidated Shareholder Claim (Quinn Emanuel & Phi Finney McDonald)	FIIG (ASIC)	Medibank (OAIC)
COURT	**Federal Court of Australia, Victorian Registry (VID64/2023)**	**Federal Court of Australia, Victorian Registry (VID256/2023)**	**Supreme Court of Victoria (SECI 2023 01227)**	**Federal Court of Australia, Queensland Registry (QUD144/2025)**	**Federal Court of Australia, Victorian Registry (VID497/2024)**
Type of proceeding	**Class action**	**Class action**	**Class action**	**Breach of s912A Corporations Act**	**Breach of s13G Privacy Act**
Measures alleged to be required (all, or alternatively, some of the following)					
Authentication and Access					
Multi-factor authentication	✓	✓[1]	✓	✓	✓
Implement appropriate password complexity for user accounts including preventing insecure or common passwords and re-use of passwords	×	×	✓	✓	✓
Least privilege controls: users can only access data required to perform their role	✓	✓[2]	✓	×	✓
Just-in-time controls: users can only access data when they needed to use it to perform their role (ie, no standing privileges).	✓	×	×	✓	✓
Access privilege change control: restrictions on a person's ability to upgrade or expand / escalate their access privileges	✓	×	×	×	✓
Remote access is managed	×	×	✓	✓	✓
Users, devices and other assets are authenticated commensurate with the risk of the transaction (including authenticating users to sensitive or critical information assets once inside a network perimeter)	×	×	✓	✓	✓
Separate administrative accounts are used for privileged access to accounts and are not used for non-privileged activities	×	×	×	✓	×
Disabling legacy and insecure authentication protocols	×	×	×	✓	×
Network segmentation					
Systems are partitioned into segments or sub-networks with unique security controls, including utilising jump boxes[3] (to help prevent lateral movement)	✓	×	✓	×	×
Monitoring for lateral movement within the network	×	×	✓	×	×
Controls to prevent a person who has gained access to the network (particularly external party credentials) from accessing additional credentials within those networks	×	×	✓	×	✓
Patch management system	✓	×	×	✓[4]	×

[1] Any party requesting access to personal information via the internet required to authenticate using a valid security credential and/or multi-factor authentication.

[2] More specifically, identifying document personal information (eg, government-issued identifiers) should not be accessible via an API on the internet, except in respect of authorised specific access for legitimate business purposes and such access restricted to the person's authorised internet IP address.

[3] Jump boxes are hardened computer servers that operate as a controlled bridge / means of access between two network areas.

	Medibank Consolidated Consumer Claim (Baker McKenzie)	Optus Consumer Claim (Slater & Gordon)	Medibank Consolidated Shareholder Claim (Quinn Emanuel & Phi Finney McDonald)	FIIG (ASIC)	Medibank (OAIC)
COURT	**Federal Court of Australia, Victorian Registry (VID64/2023)**	**Federal Court of Australia, Victorian Registry (VID256/2023)**	**Supreme Court of Victoria (SECI 2023 01227)**	**Federal Court of Australia, Queensland Registry (QUD144/2025)**	**Federal Court of Australia, Victorian Registry (VID497/2024)**
Type of proceeding	**Class action**	**Class action**	**Class action**	**Breach of s912A Corporations Act**	**Breach of s13G Privacy Act**
Encryption controls on relevant information (including passwords)	✓	✓	✓	✗	✓
Monitoring and Detection					
Systems (including firewalls and vulnerability scanning) to detect and monitor for malicious, unusual or unwanted traffic or behaviour (including threat actors)	✓[5]	✓	✓	✓	✓
Up to date cyber threat intelligence to collect, process and analyse system data to identify, monitor and anticipate unauthorised access to systems and strategies and tactics of threat actors	✓	✗	✓	✓	✗
Configurations such as security configurations of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed	✗	✗	✓	✗	✗
Application controls to protect against malicious code executing on systems	✓	✗	✗	✗	✗
Systems and controls to prevent extraction of substantial volumes of data including personal information	✗	✓	✓	✓	✓[6]
Security mechanisms, service levels and service requirements of network services identified, implemented and monitored, and included in network services agreements (whether services provided in-house or outsourced)	✗	✗	✓	✗	✗
Testing					
Monitoring, review and testing of security controls to identify issues including lack of MFA and potential for unauthorised access or access of additional credentials	✓	✓	✓	✗	✓
Change management processes to ensure that system changes do not result in failure of other security measures (including MFA and extraction prevention)	✗	✓	✗	✗	✓
Monitoring, review and testing of security controls to identify failures of systems and processes	✗	✓	✓	✓	✓
Regular audits and / or testing to ensure that third party contractors with access to networks are complying with security policies	✗	✗	✗	✗	✓
Systems to delete personal information no longer required to be held	✓	✓	✓[7]	✗	✗
Undertaking crown jewel analysis to identify critical applications and data and employing additional measures to protect that data	✓	✗	✗	✗	✗
Cyber incident response plan which is accessible and communicated to all employees, addressing the action to be taken, key roles and responsibilities of personnel, regulatory notification requirements, and incident detection, analysis and response	✗	✗	✗	✓	✗
Training, supervising, auditing and correcting staff to ensure secure handling of software and hardware tools used to gain access to systems and networks.	✓	✗	✗	✓	✗

[4] Including a patching plan to identify available patches and software updates, a practice of ensuring patches and software updates are applied within specified timeframes; a practice of updating all operating systems to at least a version currently supported by vendor; and applying additional compensating controls to systems which cannot be updated or patched, to control the increased risk of compromise.

[5] In addition, systems to react in real-time to block or prevent such malicious, unusual or unwanted traffic or behaviour.

[6] 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.

[7] Reasonable steps are taken to destroy or de-identify personal information where it is no longer needed for a permitted purpose.