Comparative review of Australian data breach class actions

	Medibank consumer claim (Baker McKenzie)	Medibank consumer claim (Slater & Gordon)	Optus consumer claim (Slater & Gordon)	Medibank shareholder claim (Quinn Emanuel)
Court	Federal Court of Australia, Victorian Registry	Federal Court of Australia, Victorian Registry	Federal Court of Australia, Victorian Registry	Supreme Court of Victoria
Causes of action				
Breach of contract	✓	✓	✓	×
Breach of confidence	✓	×	×	×
Negligence	×	✓	✓	×
Misleading or deceptive conduct	✓	✓	✓	×
Breach of continuous disclosure obligations	×	×	×	✓
Loss and damage	Damages for *distress, embarrassment and anxiety* of having their personal information published on the dark web.	Damages for: • *distress, frustration and/or disappointment* resulting from the disclosure of the applicants' personal information; and • the cost and time associated with addressing the consequences of the Medibank data breach.	Damages for: • *emotional distress* resulting from the disclosure of the applicants' personal information; and • the cost and time associated with addressing the consequences of the Optus data breach.	The plaintiff claims loss by reference to Medibank's 18% share price drop and pleads market-based causation and, in the alternative, reliance.
Applicable regulatory requirements	• Privacy Act,[i] s13A[ii], s15[iii], APPs[iv] 1.2, 1.3, 1.4, 6.1, 6.2, 11.1 and 11.2 and NPPs[v] 2.1, 2.2, 4.1, 4.2 and 5 • HR Act (Vic),[vi] ss11(2), 21, and HPP 2.1, 2.2, 4.1, 4.5, 5.1 • HRIP Act (NSW),[vii] ss11(2), 11(3) and HPP 4, 5.1(a)-(b), 5.1(c), 10(1)	• Privacy Act, s15 and APPs 1.2, 11.1 and 11.2.HR Act (Vic), s11(1) and HPP 4.2 • HRPA Act (ACT), s6(1) and HPP 4.2 • PHIPS Act (Cth), s92(1) and 94 • CPS 234, paragraphs 15, 17, 21, 23, and 27 • ACL, ss18, 29(1) and 34	• Privacy Act, s15 and APPs 1.2, 11.1, 11.2 • TIA Act,[xiii] ss187A 187AA, 187BA, 187C • ACL, ss18, 29(1) and 34	• PHIPS Act (Cth), s92 • CPS 234, paragraphs 13, 15, 16, 17, 21, 22, 23, 27–34

	Medibank consumer claim (Baker McKenzie)	Medibank consumer claim (Slater & Gordon)	Optus consumer claim (Slater & Gordon)	Medibank shareholder claim (Quinn Emanuel)
	• HRPA Act (ACT),[viii] s6(1), and HPP 2, 4.1(a), 4.3(2) and 9(1) • PHIPS Act (Cth),[ix] s92(1) • CPS 234,[x] paragraphs 15, 21, 36 • ACL,[xi] ss4, 18, 29 or TPA,[xii] ss51A, 52, 53.			
Specific industry standards and practices the plaintiff alleges should be met	Alleges that the appropriate practice includes ISO27001,[xiv] NIST CSF,[xv] Essential Eight[xvi] and ISM.[xvii]	None	None	None
Measures alleged to be required				
Authentication and access				
Multi-factor authentication	✓	✓	✓[1]	✓[2]
Least privilege controls: users can only access data required to perform their role	✓	See Just in Time requirement	✓[3]	×
Just-in-time controls: users can only access data *when* they need to access it to perform their role (ie no standing privileges)	✓	✓[4]	×	×
Access privilege change control: restrictions on a person's ability to upgrade or expand / escalate their access privileges	✓	×	×	×

[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] Change management systems in place that ensure new or modified remote access to systems and networks always requires multi-factor authentication.

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

[4] Security measure required for systems and networks that held personal information relating to health claims and services.

	Medibank consumer claim (Baker McKenzie)	Medibank consumer claim (Slater & Gordon)	Optus consumer claim (Slater & Gordon)	Medibank shareholder claim (Quinn Emanuel)
Network segmentation				
Systems are partitioned into segments or sub-networks with unique security controls, including utilising jump boxes[5] (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 those with external party credentials) from accessing additional credentials within those networks	×	✓	×	×
Patch management system	✓	×	×	×
Encryption controls on relevant information	✓	×	×	×
Monitoring and detection				
Systems (including firewalls) to detect and monitor for malicious, unusual or unwanted traffic or behaviour (including threat actors)	✓[6]	✓[7]	✓	✓[8]
Up-to-date cyber threat intelligence to collect, process and analyse system data to identify, monitor and anticipate	✓	×	×	×

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

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

[7] In addition, swift response to any such alerts triggered by the detection and monitoring.

[8] Including endpoint detection and response system to identify malicious software.

	Medibank consumer claim (Baker McKenzie)	Medibank consumer claim (Slater & Gordon)	Optus consumer claim (Slater & Gordon)	Medibank shareholder claim (Quinn Emanuel)
unauthorised access to systems and strategies, and tactics of threat actors				
Application controls to protect against malicious code executing on systems	✓	×	×	×
Systems and controls to prevent extraction of substantial volumes of data, including personal information	×	✓	✓	✓
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	×	×	✓	×
Systems to delete personal information no longer required to be held	✓	✓	✓	×
Undertaking crown jewel analysis to identify critical applications and data, and employing additional measures to protect that data	✓	×	×	×
Training, supervising, auditing and correcting staff to ensure secure handling of software and hardware tools used to gain access to systems and networks	✓	×	×	×

	Medibank consumer claim (Baker McKenzie)	Medibank consumer claim (Slater & Gordon)	Optus consumer claim (Slater & Gordon)	Medibank shareholder claim (Quinn Emanuel)
Impugned representations or communications				
Express contractual terms:	Contractual terms contained in health insurance policies and direct debit agreements stated Medibank / AHM would: • comply with its privacy policy and terms and conditions; • ensure all information was stored securely and only for so long as required; • keep financial information confidential; and • use personal information provided to it in support of insurance claims in accordance with the privacy policy and terms and conditions.	Contractual terms contained in the relevant 'Guide', 'Terms' and Privacy Policy stated that Medibank / AHM would: • comply with its privacy policy; • ensure all information was stored securely and only for so long as required; and • comply with its legal obligations in handling information.	Contractual terms contained in consumer and small and medium business terms of service stated Optus would: • comply with its privacy policy; • provide services and ancillary services with due care and skill; and • comply with its legal obligations in handling information.	No breach of contract alleged.
Implied contractual terms:		Implied terms to the effect that Medibank would ensure all information was stored securely and only for so long as required and comply with its statutory obligations.	Implied terms to the effect that Optus would comply with its privacy policy and legal obligations in handling information.	
Representations allegedly made by the defendant:	The applicant claims that Medibank / AHM made implied representations in its *marketing and policy literature* that it would: • comply with applicable regulatory obligations and policies in place; and • maintain appropriate systems.	The applicant claims that Medibank made representations in its *customer terms and on its website* regarding the standards and sufficiency of its cyber controls.	The applicant claims that Optus made representations: • in its *marketing and policy literature* to the effect that it complied with its privacy policy and legal obligations in handling information; and • on its website that it treated personal information with great care and stored it securely.	There is currently no claim for misleading or deceptive conduct based on express or implied representations. Instead, the plaintiff alleges Medibank failed to disclose material information, being that its systems and controls were inadequate under CPS 234 and that there was a serious risk of a cyber breach.

	Medibank consumer claim (Baker McKenzie)	Medibank consumer claim (Slater & Gordon)	Optus consumer claim (Slater & Gordon)	Medibank shareholder claim (Quinn Emanuel)
Relief sought by the plaintiff:	• Damages (general contractual and under the ACL / TPA) • Equitable compensation • Aggregate damages for the whole of the group members under ss33Z(1)(e), (f) and/or (g) of the *Federal Court of Australia Act 1976* (Cth) • Mandatory injunction under ss80W and / or 98 of the Privacy Act to destroy or de-identify personal information Medibank / AHM no longer needs • Declarations that Medibank / AHM breached ss18 and / or 29 of the ACL, and / or alternatively ss52 and 53 of the TPA	• Damages (breaches of contract, regulatory requirements, duty of care and under the ACL) • Mandatory injunction under s80W of the Privacy Act and s121 of the RPSP Act[xviii] to delete or de-identify appropriate information • Declarations that Medibank contravened certain regulatory requirements	• Damages (breaches of contract, regulatory requirements, duty of care, and under the ACL) • Mandatory injunction under ss80W and / or 98 of the Privacy Act to destroy or de-identify appropriate information • Declarations that Optus breached certain regulatory requirements	Damages as a result of the continuous disclosure contraventions will depend on: • a class member's timing of the acquisition / sale of shares (and whether they continued to hold their shares); and • the 'true value' of the shares / price that would have prevailed but for the breach of Medibank's continuous disclosure obligations.

[i] *Privacy Act 1988* (Cth) (the ***Privacy Act***).
[ii] Section 13A required an organisation not to do an act, or engage in a practice, that breached an NPP.
[iii] Section 15 requires an organisation not to do an act, or engage in a practice, that breaches an APP.
[iv] Australian Privacy Principles.
[v] National Privacy Principles, the predecessor to the Australian Privacy Principles.
[vi] *Health Records Act 2001* (Vic) (the ***HR Act*** **(Vic)**).
[vii] *Health Records Information and Privacy Act 2002* (NSW) (the ***HRIP Act*** **(NSW)**).
[viii] *Health Records (Privacy and Access) Act 1997* (ACT) (the ***HRPA Act*** **(ACT)**).
[ix] *Private Health Insurance (Prudential Supervision) Act 2015* (Cth) (the ***PHIPS Act*** **(Cth)**).
[x] Prudential Standard CPS 234 Information Security (the ***CPS234***).
[xi] Schedule 2 of the *Competition and Consumer Act 2010* (Cth) (the ***ACL***).
[xii] *Trade Practices Act 1974* (Cth) (***TPA***) (the predecessor to the ACL).
[xiii] *Telecommunications (Interception and Access) Act 1979* (Cth) (the ***TIA Act***).
[xiv] International Organization for Standardization international standard to manage cybersecurity.
[xv] National Institute of Standards and Technology Cybersecurity Framework.
[xvi] Essential Eight Maturity Model published by the Australian Cyber Security Centre.
[xvii] Information Security Manual produced by the Australian Cyber Security Centre.
[xviii] *Regulatory Powers(Standard Provisions) Act 2014* (Cth).