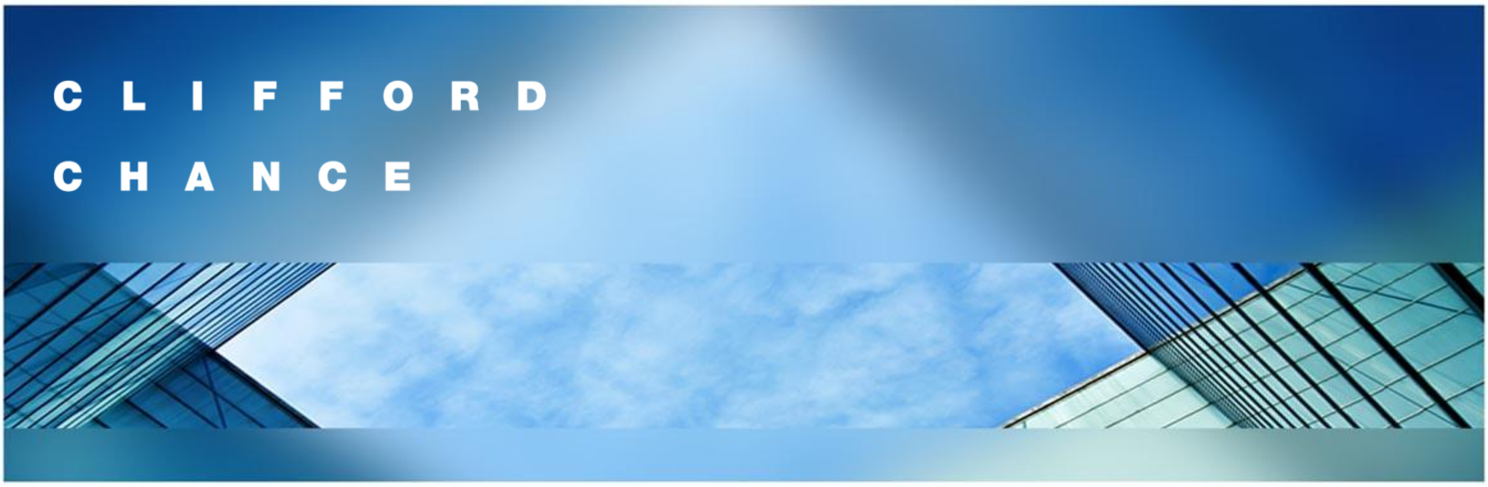

DATA AND CYBER LITIGATION + DAMAGES.

In Australia and the UK, data or cyber breaches have been followed by group litigation on behalf of customers and/or shareholders. It is not yet clear how damages will be assessed in these cases. We analyse the current position to assist defendants in considering the live issues.

DAMAGES IN CLASS ACTIONS & GROUP CLAIMS

There are currently several data breach class actions in the early stages of litigation or under investigation in Australia - these claims concern alleged breaches of the Privacy Act as well as negligence and Australian Consumer Law claims. The claims are brought by customers whose data has been the subject of the breach or by shareholders of the company who held shares prior to and around the time of the breach. In November 2022, we wrote about the challenges for damages claims in data or cyber breach group claims. The conclusion was that mass claims will have to grapple with uncertainty around the appropriate measure of loss or damage for individuals arising from a data breach.

Revisiting the position a year later, those uncertainties remain. Similarly, in the UK, a number of recent Court decisions have highlighted the difficulty in bringing mass data claims on an opt-out basis, not least due to the difficulties of calculating loss and damage on a class-wide basis.

Key issues

- Data and cyber breaches are being followed by private litigation, in particular class actions and group litigation
- The way in which a Court will quantify loss or damage for claims arising from data or cyber breaches is unclear
- Claims can take the form of actions by customers and/or actions by shareholders
- Economic loss claims have limitations given the difficulty of identifying more than nominal individual loss
- Non-economic loss claims may turn on their facts and could be difficult to prosecute in a group context

Customer claims

There are numerous unanswered questions as to how loss and damage should be quantified for individuals subject to a data breach.

For economic loss claims, the Office of the Australian Information Commissioner has previously adjudicated representative claims arising from a release of immigration detainee's private information by the Department of Home Affairs. The people impacted were each required to individually submit information proving their loss or damage, with estimated economic loss claims in the range of $500 to $20,000 for more extreme loss or damage from the data breach.

Non-economic loss claims may prove more difficult. For example, if you have to replace your driver licence and your bank cards, should you be able to recover for any 'time' cost or inconvenience associated with this? If your data is stolen and kept on the dark web but you don't know it is there or there is otherwise no misuse of that data, has any loss been suffered? Do you have to wait until your identity is stolen and misused to bring a claim? Is the appropriate form of relief declaratory requiring rectification of data storage procedures and defences to cyber-attacks?

A recent judgment from the Federal Court of Australia in the *Ruby Princess* class action may be a further aid to illustrate the challenges with non-economic loss claims by customers. In that case, the Court found that the applicant customer could recover distress and disappointment damages of around $4,000 but could not recover non-economic loss for psychological injury or other personal injury. Whilst that case was about a cruise ship where passengers contracted covid-19 nevertheless the legal basis on which the non-economic loss claims were brought were the Australian Consumer Law and negligence (which are routinely pleaded in data breach class actions).

In the UK, claimants have had difficulty seeking to use the representative action to bring claims for breaches of data protection legislation following the UK Supreme Court's decision in *Lloyd v Google* in 2021. In that case, the Supreme Court concluded that the claim failed the "same interest" test because it would require an individualised assessment of damages. Earlier this year, the High Court struck out a data claim brought against Google by Andrew Prismall on behalf of a class of approximately 1.6 million patients of the Royal Free London NHS Foundation Trust for misuse of private information following the transfer of medical records to DeepMind (part of the Google group of companies). In that case, the Court found that the class would only meet the bar for having the "same interest" in the claim if the claims were to be assessed on a "lowest common denominator" basis (i.e. the irreducible minimum level of harm suffered by all members of the class) and that damages assessed on that basis would be too trivial to succeed. The High Court's decision in *Prismall v Google* is pending appeal, but it seems for now that claimants will have to show that the data and facts in issue mean that the class as a whole has a more than *de minimis* claim for damages. That is most likely where the data is sensitive and/or where there has been egregious misuse.

Given the difficulties of using the representative action regime to bring mass data claims, creative claimants may look to make use of the UK's other opt-out class actions regime in the Competition Appeal Tribunal (**CAT**). However, in the case of *Gormsen v Meta*, the CAT ordered a stay, rather than certifying a collective action arising from Meta's alleged abuse of its dominant position by making users' access to Facebook contingent on giving it permission to collect, share and otherwise process users' personal data without payment. The CAT was not persuaded that the proposed class representative (**PCR**) had demonstrated a realistic prospect of establishing loss on a class-wide basis. The CAT instead ordered a stay to allow the PCR more time to re-formulate its loss methodology, explaining that the PCR only needed to show how disputed points could and would be addressed, noting that answers to these questions do not need to be provided at the certification stage. If the PCR could not demonstrate how these points would be addressed, the CAT stated it would reject the application as it saw no point in permitting untriable cases to proceed to trial.

Shareholder claims

After a data breach, the Australian Prudential Regulation Authority required Medibank to hold an additional $250 million in capital. Greater capital adequacy (a requirement for insurance and financial services) may give a degree of comfort to investors after a data breach. However, when it comes to damages, investors would more typically claim that an undisclosed systemic issue or failure to prevent a data breach meant the share price was artificially inflated (not that the company was inadequately capitalised).

A systems or failure to prevent case will be relatively novel territory for economic loss claims, as most 'stock-drop' shareholder claims in Australia rely on failure to disclose allegedly inaccurate financial information. An event study expert might come along and say that had a systemic data privacy issue been disclosed (giving rise to the risk of regulatory action) then the market would have reacted and adjusted the share price. This perhaps presumes a counterfactual where a listed company identifies and discloses that it has inadequate data privacy systems (surely a red rag to hackers).

Similarly, in the UK, it is theoretically possible that claimants may look to use the securities litigation regime under section 90A of the Financial Services Markets Act 2000 to bring a claim against an issuer where the issuer is said to have made an allegedly false or misleading statement to the market or made a material omission as to its data protection systems, which are later shown to be defective through a data breach, causing the share price to fall. However, we are not currently aware of any such claims being litigated in England and Wales, and any such claims would need to establish that the claimants relied on the relevant statement or omission when buying, holding or selling the relevant securities.

These types of difficulties calculating loss may present challenges for settling data breach class actions, especially where the monetary bounds of potential claims are an unknown.

CLIFFORD CHANCE

CONTACTS

Naomi Griffin
Partner

T +61 2 8922 8093
E Naomi.Griffin@cliffordchance.com

Jason Epstein
Senior Associate

T +44 207006 3996
E Jason.Epstein@cliffordchance.com

Maxine Mossman
Partner

T +44 207006 4204
E Maxine.Mossman@cliffordchance.com

Angela Pearsall
Partner

T +61 2 8922 8007
E Angela.Pearsall@cliffordchance.com

Samantha Ward
Partner

T +44 207006 8546
E Samantha.Ward@cliffordchance.com

Kate Scott
Partner

T +44 207006 4442
E Kate.Scott@cliffordchance.com

Andrew Murn
Counsel

T +61 2 8922 8510
E Andrew.Murn@cliffordchance.com

Stella Cramer
Partner

T +65 9011 1196
E Stella.Cramer@cliffordchance.com

Ling Ho
Partner

T +852 2826 3479
E Ling.Ho@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, Level 24, 10 Carrington Street,

Sydney, NSW 2000, Australia

Liability limited by a scheme approved under professional standards legislation

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.