Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

UK Group Data Breach Claims Pose Big Financial Risks

By **Annabel Gillham, Ioanna Lamprinaki and Rayhaan Vankalwala**
March 12, 2020, 4:20 PM EDT


Annabel Gillham


Ioanna Lamprinaki


Rayhaan Vankalwala

The U.K.'s data protection regulator, the Information Commissioner's Office, has announced an intention to issue some big-hitting fines, some edging well over £100 million. The theoretical threat of significant fines under the General Data Protection Regulation has become a reality for some businesses (and their insurers).

But that may not be the end of the story.

How concerned should businesses be that adverse regulatory findings will be used as a springboard for mass claimant lawsuits for damages — akin to class actions?

In this article, we explore how these lawsuits are arising in the U.K., and the potential financial exposure and the risk of doomsday outcomes for defendant organizations.

U.K. Group Litigation: The Headline Cases

Recent high-profile cases consider the procedural options for launching data breach collective actions, paving a more precise (and arguably far less bumpy) road map for future mass claims.

In Various Claimants v. WM Morrison Supermarkets,[1] a claim which predates the GDPR, over 5,000 claimants are seeking compensation from the well-known U.K. supermarket chain. The claims arise from a data breach in which a disgruntled employee posted colleagues' payroll information online in 2014.

On Oct. 4, 2019, the English High Court gave the green light[2] to a group claim brought by thousands[3] of claimants against British Airways PLC arising from the data security incident involving the personal data of approximately 500,000 customers in 2018. This claim was filed just months after the ICO issued a £183.39 million fine against BA.

In a third case, Lloyd v Google Inc.,[4] the claimant has sought to bring a

representative action on behalf of a class of 4.4 million iPhone users. The substance of the complaint relates to Google tracking iPhone users' internet activity, without consent, for commercial purposes. The claimant advanced a figure of £750 per member of the class at an early stage in proceedings, making Google's estimate of its potential liability between £1 billion and £3 billion.

These cases signal challenging times ahead for defendant organizations:

- Companies can be vicariously liable for the personal data infringements caused by the actions of rogue employees;

- Claimants can sue for loss of control of data, even if they suffer no financial loss or distress due to the breach, provided that the loss of control was not trivial; and

- "Class action" style proceedings for data breaches are far more viable than in the past.

Coupled with the range of litigation funding options and the keen appetite of claimant law firms to take on mass litigation, the signs point to a new era of data breach collective actions in the U.K.

What are the routes to group litigation?

Claimants in the U.K. have primarily relied on two procedural regimes to bring high profile data breach class-actions: the group litigation order, or GLO, (where claimants opt in) and the representative action (where — broadly speaking — individuals with the same interest as the claimant may theoretically form part of a claim unless they opt out).

Launching a representative action has traditionally been far more challenging than seeking a group litigation order; the English courts have (until now) construed the same-interest test very narrowly.

The GLO Action

A GLO action is essentially a case management process for multiple claimants. The claimants must show that their claims share "common or related issues of fact or law"[5] and must identify themselves and register by a specific deadline. Given that GLO claimants share common — not necessarily identical — issues to be determined, the court will take this into account when deciding damages.

The Representative Action

Unlike GLOs, representative action claims do not require the identification of all represented individuals. The mechanism effectively provides for an opt-out process whereby identifiable individuals with the same interest can, in certain circumstances, form part of the class unless they opt out.

To launch a representative action claim, the relevant representative must have the same interest in the claim as the individuals s/he seeks to represent.[6] The same-interest test has, until recently, been a high hurdle for claimants to clear and was rarely met. However, the Court of Appeal in the Lloyd case has lowered that hurdle.

At first instance, the High Court[7] found that Lloyd did not satisfy the same interest test because the number, nature, extent and impact of the breaches on individual users varied dramatically. The High

Court noted that it was impossible to identify all members of the class or to verify those that came forward to claim compensation.

The Court of Appeal reversed the High Court's decision. It favored the claimant's argument that the represented claimants would share the same interest if they had all lost control over their data. In this case, the argument was run that Google had taken browser-generated information (which is something of value), without individuals' consent, in the same circumstances, during the same period.

The court further held that the members of Lloyd's class were identifiable (although not yet identified) because (1) every affected person would, in theory, know whether or not they satisfy the conditions of the class; and (2) Google itself would be able to identify members of the class.

As such, the court decided that, in principle, damages are capable of being awarded for loss of control of data even if there is no pecuniary loss and no distress, provided that the loss of control of data is more than trivial.

We anticipate that Google will appeal the decision to the Supreme Court. However, this does not diminish the decision's profound significance, and its potential impact in giving rise to similar claims, at least in the short term.

What other implications arise from recent cases?

The Morrisons and Lloyd cases may well have fueled the appetite for data breach group actions by clarifying the procedural aspects of launching such claims. They also expanded the scope of liability and damages in data breach class actions.

Vicarious Liability

In Morrisons, the Court of Appeal held that employers could be vicariously liable for the misuse of personal data by a rogue employee, even though:

- Morrisons was found to have had robust data protection programs in place;
- Morrisons was a victim of the rogue employee's actions; and
- The employee committed the data breach on his personal computer at his home.

The Court of Appeal's reasoning was that there was an unbroken thread, which linked the employee's role to the data breach; Morrisons was vicariously liable for the breach.

Morrisons appealed the Court of Appeal's decision, and the Supreme Court's decision is pending.

No Need to Prove Pecuniary (Financial) Loss or Distress

In Lloyd, the Court of Appeal held that, in principle, damages can be awarded for the loss of control of personal data, even if the data breach caused no financial loss or distress to the victims, provided that the loss of control was not trivial.

The Court of Appeal made explicit reference to the recitals to the GDPR, noting that the loss of control of personal data is an example of the kind of damage that a data breach may cause to individuals.[8] The court also considered that, under Section 13 of the Data Protection Act, a person who suffers damage due to a breach of data protection legislation is entitled to compensation.

While the case was decided under the old Data Protection Act of 1998, the provisions of the GDPR and Data Protection Act of 2018 are largely the same in this regard (Article 82 of the GDPR includes a right to compensation for "any person who has suffered material or non-material damage").

More importantly, the definition of "damage" in this context under the Data Protection Act of 2018 (per Section 169 of that act) includes both financial loss and damage not involving financial loss, potentially encompassing loss of control.

Awarding Damages

Although no one can yet be sure how damages will be calculated in these cases, we predict that damages awarded in the U.K. collective actions will, in general, be lower than their U.S. equivalents. The estimated quantum in the Lloyds case is perhaps an extreme example — given the number of users in the class. Contrary to the U.K., U.S. class actions tend to be tried in front of a jury, which may well be less predictable when it comes to damages.

Furthermore, in GLO cases, the court would likely take into consideration the individual circumstances of each claimant, and, as a result, the damages awarded may vary. On the other hand, in representative action claims, we expect that there would be a uniform amount of compensation awarded to each claimant.

Conclusion: A New Era of Data Breach Claims?

Recent decisions in the English courts appear to make it easier for victims of a data breach to bring class actions against defendant companies. Consequently, these companies may find themselves liable for potentially eye-watering sums in addition to the fines they may already have to pay under the GDPR.

This is particularly true considering the Court of Appeal's decision in Lloyd. The Court of Appeal's decision (subject to further appeal) appears to make it significantly easier for victims of a data breach to bring opt-out style class actions, with a low threshold for establishing the damage that such victims must have suffered. This is a stark turnaround from the High Court's decision at first instance.

While the level of damages per claimant may not be particularly high, this will be of little consolation where group actions are brought by a class of hundreds of thousands, if not millions, of individuals. In light of this, some businesses may be considering purchasing insurance to mitigate their potential liabilities. As the Court of Appeal in Morrisons put it:

There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees. […] The fact of a defendant being insured is not a reason for imposing liability, but the availability of insurance is a valid answer to the Doomsday or Armageddon arguments.[9]

Annabel Gillham is a partner and Rayhaan Vankalwala and Ioanna Lamprinaki are associates at Morrison & Foerster LLP.

[1] Various Claimants v. WM Morrison Supermarkets [2018] EWCA Civ 2339 – http://www.judiciary.uk/wp-content/uploads/2017/12/morrisons_approved_judgment.pdf.

[2] S. Weaver & Ors v. British Airways plc, Claim Number BL-2019-001146, Group Litigation Order – https://www.judiciary.uk/wp-content/uploads/2019/10/Weaver-ors-v-British-Airways-PLC-sealed-order.pdf.

[3] The Belfast Telegraph: British Airways customers allowed to bring data breach compensation claims – https://www.belfasttelegraph.co.uk/news/uk/british-airways-customers-allowed-to-bring-data-breach-compensation-claims-38563836.html.

[4] Richard Lloyd v. Google LLC [2019] EWCA Civ 1599 – https://www.bailii.org/ew/cases/EWCA/Civ/2019/1599.html.

[5] Civil Procedure Rules: 19.11 – https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part19#19.11.

[6] Civil Procedure Rules: 19.6 – https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part19#19.6.

[7] Richard Lloyd v. Google LLC [2018] EWHC 2599 (QB) – https://www.judiciary.uk/wp-content/uploads/2018/10/lloyd-v-google-judgment.pdf.

[8] General Data Protection Regulation (2016/679) – https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[9] Various Claimants v WM Morrison Supermarkets [2018] EWCA Civ 2339 at paragraph 78 http://www.judiciary.uk/wp-content/uploads/2017/12/morrisons_approved_judgment.pdf.