COVINGTON

EasyJet Latest Firm to Face UK Data Breach "Class Action"

June 8, 2020

Class Actions

On 19 May 2020, easyJet announced that personal data of approximately 9 million customers worldwide had been unlawfully accessed by third parties in a "highly sophisticated cyber-attack".

Data stolen by the cyber-attackers includes credit card details of 2,000 of the affected customers and, for most other customers, travel details such as departure and arrival dates/times, email addresses and other contact information requested by easyJet when making a booking.

Reports suggest that easyJet first knew of the cyber-attack in January 2020, and started notifying affected customers in April 2020 following an investigation into the scope of the breach. With a swiftness reminiscent of U.S. plaintiff class action firms, on 22 May 2020, UK law firm PGMBM issued a claim in the London High Court, and widely publicised that it would be seeking damages of up to £18 billion on behalf of easyJet's impacted customers. PGMBM have said that they intend to send easyJet a letter of claim in early June 2020.

The claim is part of a growing trend of class actions brought upon the heels of a cyber-attack. Just as in the world of antitrust, regulatory investigations and administrative fines are now only one source of legal exposure that a victim of a cyber-attack should expect.

What Might A Group Claim Against easyJet Look Like?

The claim is described by PGMBM as a "class action", but what the law firm is actually seeking is a "Group Litigation Order", which would allow it to combine claims together, and to conduct them as a single group action. A Group Litigation Order would proceed on an "opt-in" basis, which means that affected customers would have a set period of time to opt into the claim (as opposed to an "opt-out" class action, in which all members of a class are caught, regardless of their involvement). The claim in this case was issued on behalf of 43 claimants and PGMBM hope to attract many thousands or millions of affected customers to join.

These claims typically allege breaches under the Data Protection Act 2018 ("**DPA 2018**") and the EU General Data Protection Regulation (the "**GDPR**"), misuse of private information, and breach of confidence on behalf of affected customers. PGMBM has publicised that affected customers can claim compensation under Article 82 of the GDPR for "inconvenience, distress, annoyance and loss of control" of their data. The question of what constitutes personal data or private information, which enables these cases to get off the ground, is expansive, as recently demonstrated by the case of *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) concerning automated facial recognition software applied to CCTV recordings (see our report here).

The defendant normally looks to show that it took appropriate and proportionate measures to manage and defend against the risk of a security breach, thereby demonstrating compliance with Article 32 of the GDPR. In this case, easyJet has also said that "there is no evidence that any personal information of any nature has been misused", going to the question of quantum of damages. However, defendants also need to factor in compensation claims based simply on the loss of control over affected customers' data.

easyJet is the second British airline in recent times to fall victim to a cyber-attack and face a group action in the English High Court as a result. In 2018, British Airways suffered a data security breach that affected 430,000 customers. The same law firm, PGMBM (known at the time as SPG Law), launched a similar group action against British Airways which, since 4 October 2019, is also proceeding under a Group Litigation Order.

Unusually, in that case, it was British Airways that applied for the Group Litigation Order, on the basis that costs, strategy and procedural matters would be more streamlined as a result, rather than proceeding with multiple separate claims.

In the British Airways case, potential claimants were given 15 months to opt in. As the easyJet breach is reported to have affected more individuals, the opt-in period may be even longer.

Similarly, *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12, in which the UK Supreme Court ultimately held that Morrisons was not vicariously liable for a data breach deliberately perpetrated by an employee (which we have previously reported on here), proceeded under a Group Litigation Order, where around 10% of the class of 100,000 potential claimants opted in to that action. This suggests that the take up of such cases could be relatively low. PGMBM has reportedly indicated that it has offered conditional fee arrangements to over 6,000 claimants, with approximately 25,000 easyJet customers interested in joining the group action so far.

The other structural option for these kinds of claims is a representative action. This was used in the landmark case of *Richard Lloyd v Google LLC* [2019] EWCA Civ 1599 (*"**Lloyd**"*) (see our summary of the Court of Appeal decision here; the case is now on appeal to the UK Supreme Court). Unlike a Group Litigation Order, a representative action is a form of "opt-out" class action, meaning that all affected individuals who meet the eligibility criteria are brought into the class of claimants unless they actively opt out, and are represented by a lead claimant (in that case, Mr Lloyd). The number of claimants represented in a representative action is therefore normally higher than under a Group Litigation Order.

However, claimants under the representative action regime must have the "same interest" in bringing a case, meaning that their claims must proceed on an identical basis and they will be entitled to the same level of damages. Under a Group Litigation Order, each claimant can pursue its own claim and its own individual damages.

Group actions such as these are not only an English phenomenon. In Germany, the Federal Court of Justice has recently referred a data breach claim brought by a consumer group against Facebook to the European Court of Justice, to determine the extent of the GDPR provisions allowing consumer groups to bring cases on behalf of affected individuals. That decision could significantly alter the type and number of claims that businesses that experience a data breach can expect to face in the future.

What Damages Could Be Claimed?

The case law on damages is evolving. Whereas claimants used to have to show financial loss to claim under the Data Protection Act 1998 ("**DPA 1998**") (which was superseded by the DPA 2018), following the leading judgment in *Google Inc v. Vidal-Hall & Ors* [2015] EWCA Civ 311 (which we summarised here), claimants can recover compensation for any damage suffered as a result of a contravention by a data controller of the DPA 1998. This case helped to align UK law with the GDPR, which allows compensation for both "material and non-material" damage arising from a breach. This means that affected individuals could claim for "moral damages" such as distress, in addition to financial loss, in English courts.

The Court of Appeal's decision in *Lloyd* expanded this further, finding that claimants are entitled to bring a claim simply for loss of control over their personal data, which is in itself damage, for which compensation must be paid. The implications are that customers whose personal data is stolen in a cyber-attack may be entitled to damages, even where they are not claiming - or cannot show - financial loss or distress that has resulted from the breach.

In terms of the sums awarded, there is no clear guidance or standards as yet in case law as to the correct approach to be taken. Factors relevant to the court's calculation of damages include the nature of the information in question (for example, highly sensitive information has been treated as deserving of higher compensation by the English courts), the degree of harm suffered (including any psychiatric or psychological harm), the nature of the breach (deliberate hacking and misuse of powers have been found to increase the award) and the length of the breach (with some damages being calculated as a multiple of a daily rate). In this case, PGMBM's position is that affected customers could be eligible for up £2,000 each, depending on their individual circumstances.

The potential liability for defendants (and their insurers) does not end there. In this case, the UK Information Commissioner's Office (ICO) is also conducting its own investigation into the easyJet breach and has the power to impose fines of up to €20m (approximately £18m) or 4% of annual global turnover - whichever is the greater - for some breaches of the GDPR. In July 2019, the ICO announced its intention to fine British Airways £183m for a data breach. As in antitrust cases, claimants seek to rely on the regulator's findings in establishing a defendant's in-principle liability.

While the structure, content and outcomes of these cases are evolving, it is clear that cyber-attack class action damages claims are here to stay. To assist in mitigating the effect of such claims, businesses should therefore consider checking that they are adequately covered by insurance policies – in particular, general liability and/or cyber risk insurance policies.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Litigation practice:

Dan Cooper	+44 20 7067 2020	dcooper@cov.com
Louise Freeman	+44 20 7067 2129	lfreeman@cov.com
Rosie Klement	+44 20 7067 2140	rklement@cov.com
Gregory Lascelles	+44 20 7067 2142	glascelles@cov.com
Alex Leitch	+44 20 7067 2354	aleitch@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com