LAW360

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

How UK Data Breach Ruling May Rein In Insurance Claims

By **Kelly Hagedorn, Oliver Thomson and Sol Gelsomino**
(September 7, 2021, 6:43 PM EDT)

Kelly Hagedorn

Oliver Thomson

Sol Gelsomino

On July 30, the U.K. High Court of Justice handed down its judgment in Darren Lee Warren v. DSG Retail Ltd., holding that claimants will not be able to pursue personal data claims beyond those provided for in data protection legislation, when there has been a cyberattack by an unauthorized third party, and no positive action or use by the victim of that attack.

In addition, claimants who have often pled breach-of-confidence and misuse-of-private-information claims as part of such cyberattack claims — because including those claims potentially allows the recovery of after-the-event, or ATE, insurance premiums — may find themselves on the small claims track, where costs are not recoverable.

Individuals affected by data breaches typically bring low-value claims in the hope that they result in quick settlement payments. This recent decision is of commercial interest because it questions the financial viability of bringing low-value data breach claims in the first place.

If claimants cannot recover ATE insurance premiums, claimant law firms are likely to be more selective on the claims they bring, particularly given that organizations facing cyberattacks will now have stronger grounds on which to defend low value claims.

Background

DSG Retail, the operator of retail stores Currys PC World and Dixons Travel, was the victim of a cyberattack between July 24, 2017, and April 25, 2018,[1] in which the data of at least 14 million customers may have been accessed.

One of the affected customers was the claimant, Warren, whose name, address, phone number, date of birth and email address were compromised or lost.

Warren subsequently brought a claim against DSG for £5,000 (about $6,900) on account of the distress he suffered. Warren suffered neither a diagnosed personal injury nor any identifiable pecuniary loss.

The information commissioner investigated the cyberattack and found that DSG had breached Data Protection Principle 7 of the Data Protection Act of 1998, or DPA. This principle requires data controllers to take appropriate technical and organizational measures against unauthorized or unlawful processing of data.

In January 2020, the information commissioner issued DSG with a monetary penalty notice for £500,000. In doing so, it noted that DSG's culpability was striking and there was "no justification or excuse for the extent of these systemic inadequacies."

Decision of the English High Court

DSG sought summary judgment or strikeout of the claims in:

- Breach of confidence;
- Misuse of private information; and
- Common law negligence.

The court agreed with DSG, holding that each of the above claims fell to be dismissed or struck out.

The claimant also brought a fourth cause of action for breach of the DPA, specifically the statutory duty arising out of Data Protection Principle 7, which was not the subject of DSG's application. This remaining aspect of the claimant's case has now been transferred to the county court for consideration.

Breach-of-Confidence and Misuse-of-Private-Information Claims

With regard to misuse of private information, the claimant argued that:

- The compromised information was prima facie private and rendered the claimant susceptible to identity fraud; and
- In providing the information to DSG, the claimant had a reasonable expectation that his information would be adequately protected.

In short, the claimant argued that DSG's failure to implement basic security measures was tantamount to publication, and therefore misuse of his private information.

The claimant conceded that the breach-of-confidence claim was not tenable and should not have been pleaded, but the claim was still considered by the high court as it had not been formally discontinued.

It was held that in order to succeed with a claim for breach of confidence and misuse of private information, the claimant would be required to prove some form of positive conduct by DSG. Relying on a series of case law, the high court emphasized that breach of confidence imposes an obligation on a defendant not to disclose confidential information or use it in a way that is inconsistent with its confidential nature.[2]

Similarly, misuse of private information requires some form of use even if that is an unintentional use of private information. As DSG was the victim of the cyberattack it was held that DSG cannot have

purposefully facilitated the incident — there was no positive conduct on the part of DSG that amounted to disclosure or misuse.

Instead, the claim against DSG appeared to be framed as the failure to adhere to "some form of data security duty." The high court dismissed the possibility that the causes of action of breach of confidence or misuse of private information impose such a duty on data controllers, even if the information is confidential or private.

The high court also rejected the notion that DSG should be liable for the actions of a third party — in this case the criminal third-party hackers — outside of claims under the data protection legislation.

Negligence

The claimant argued that it had a prima facie case in negligence and noted that the duty under negligence is distinct from the statutory duty under Data Protection Principle 7.

The high court rejected the negligence claim on two bases:

- First, that there is no need to construct a concurrent duty in negligence when a bespoke statutory regime already exists; and
- Second, that distress alone — absent a clinically proven personal injury — is not sufficient to complete a tortious cause of action in negligence.

As noted above, the claimant brought a fourth cause of action, arising from a breach of statutory duty in the DPA. This was not the subject of DSG's application, and will be determined in the County Court.

ATE Insurance

The Department for Digital, Culture, Media and Sport recently reported that two in five businesses and a quarter of charities have reported cybersecurity breaches in the last 12 months.[3]

This equates to large numbers of potential claimants, a group that certain claimant law firms have sought to monetize. The vast majority of potential claimants are individuals who rely on financial assistance to pursue claims; individuals typically enter into no-win-no-fee agreements and firms purchase ATE insurance on behalf of their clients to protect them from having to pay the defendant's costs in the event their claims are unsuccessful.

Following the Jackson reforms, the recoverability of the costs of ATE insurance premiums from defendants was prohibited.

However, there is an exception to that general rule where a claim is brought in privacy. Claimants are still entitled to recover ATE insurance premiums from defendants in those cases. Therefore, claimants commonly bring breach-of-confidence and misuse-of-private-information claims alongside statutory claims in cases related to data breaches.

The commercial significance of the Warren v. DSG case lies in the financial impact that curtailing breach-of-confidence and misuse of private information claims will have on claimants and claimant law firms. Following this recent judgment, parties will still be able to take out ATE insurance but — most likely now

being unable to bring breach-of-confidence or misuse of private information claims — will no longer fall within the publication and privacy proceedings carveout.

Claimant law firms will now have to bear the cost of the ATE premiums, and this could render many claims economically futile.

Concluding Remarks

This judgment narrows the basis upon which claims can be made following a data breach. Protections afforded by data protection legislation have not been affected and will continue to be relied upon in data breach scenarios, but the financial viability of such claims has been brought into question.

While small claims are more likely to be affected, it will be interesting to see whether this judgment might also limit broader class actions.

This decision may also affect the allocation of claims; breach-of-confidence and misuse-of-private-information claims can be commenced in the high court but claims for breach of the Data Protection Act may be allocated to the small claims track given the typical low value of such claims, particularly where claims are for distress, such as here.

Claimants in the small claims track will not be able to recover costs in the case, and will consequently need to think very carefully about their costs exposure before commencement.

While individuals continue to be protected by data protection legislation, the ability to seek damages and to recover ATE premiums with a meaningfully reduced cost risk could now be a thing of the past.

Kelly Hagedorn is a partner, and Oliver J. Thomson and Sol Gelsomino are associates, at Jenner & Block LLP.

[1] The cyberattack therefore took place before the General Data Protection Regulation came into effect.

[2] See Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] 1 W.L.R. 1556 at [23] and Sports Direct International plc v Rangers International Football Club plc [2016] EWHC 85 (Ch) at [26].

[3] A full copy of the Cyber Security Breaches Survey 2021 report can be found here: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.