BCLP. Client Intelligent

**Insights**

# NO LIABILITY TO DATA SUBJECTS FOR LOSS OF PERSONAL INFORMATION OTHER THAN UNDER DATA PROTECTION LAWS FOR COMPANIES THAT ARE THE VICTIMS OF CYBER-ATTACKS

Aug 17, 2021

## SUMMARY

A recent High Court case examines the liability position where leaks or losses of personal data occur as a result of the actions of a cyber-attacker, rather than as a result of breaches or misuse by the data controller itself. It is a ruling which businesses will welcome, as it may narrow the types of claims which data subjects can bring against data controllers. It will not however, allow data controllers to avoid liability stemming from failures to meet statutory obligations – such as having adequate systems and controls- to protect personal data from external attack or compromise.

In *Darren Lee Warren v DSG Retail Limited [2021] EWHC 2168 (QB),* the High Court summarily struck out claims by a customer against DSG Retail Limited ('**DSG**') (operator of the 'Currys PC World' and 'Dixon Travel' brands) for breach of confidence and misuse of private information arising out of a cyber-attack that resulted in the customer's personal information potentially being leaked.

DSG had potentially failed to take reasonable steps to prevent the cyber-attack, and claims may still lie for potential breach of statutory duty under the Data Protection Act 1998 ("**DPA**"). However, the High Court held that there was no basis in law for claiming against DSG (as data controller) for breach of confidence and data misuse as these were acts committed by the (anonymous) attacker itself.

The decision is not surprising, given the Supreme Court's 2019 judgment in *Wm Morrison Supermarkets plc* that companies are not directly liable for the actions of rogue employees who deliberately leak confidential information (other than in relation to any breach of the DPA) ). If a company is not liable for its own employee, it is unlikely to be liable for a third party hacker.

## BACKGROUND

Between 2017 and 2018, cyber hackers infiltrated DSG's systems and installed malware on 5,930 point of sale terminals at the DSG stores. During this cyber attack, the personal data of around 14 million customers (including the claimant) was stolen.

In January 2020, after investigating the attack, the Information Commissioner fined DSG £500,000 for breach of the seventh data protection principle from Schedule 1 of the DPA – namely, failing to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data (**"DPP7"**).

On the back of this finding, the claimant issued a claim for damages in the amount of £5,000 against DSG as the data controller arguing that his personal information (name, address, phone number, date of birth and email address) had been compromised during the attack. He pleaded the following causes of action:

1. breach of confidence ("**BoC**");

2. misuse of private information ("**MPI**");

3. common law negligence; and

4. breach of statutory duty under the DPA.

Consequently, DSG made an application for summary judgment and/or to strike out all of the causes of action apart from the claim for statutory duty under the DPA.

## BOC AND MPI CLAIMS

The judge rejected the Claimant's contention that allowing a third party unauthorised access to personal data led to an infringement of his right to privacy and facilitated the misuse of his private information and dissemination to a third party.

Judge Saini clarified that:

- For a claim in BoC or MPI to arise in law, the defendant must have taken some positive wrongful action in relation to the information in question – typically, disclosing it to a third party or making some other unauthorised use of it – whereas, DSG itself was a passive victim and did not purposefully facilitate the cyber-attack.
- Neither BoC nor MPI impose a data security duty on holders of private or confidential information and imposing such a duty would be a 'development of law' that was contrary to existing case law authority.
- Both the claims (BoC and MPI) are concerned with prohibiting actions by the holder of information that are inconsistent with the obligation of confidence/privacy.

- With regard to a claim for MPI, 'misuse' may include unintentional use, but it still requires a 'use': there must an 'interference' by the defendant, a positive action of wrongful conduct, which falls to be justified by the Claimant.
- DSG's alleged failure to implement basic security measures to protect the claimant's information did not amount to a 'publication' of that information to the third-party hacker.

In short, the court concluded that it was not DSG that disclosed the Claimant's personal data, or misused it – damage was due to the actions of the criminal third-party hackers and therefore any liability of DSG that arose could only be under the relevant statutory regime for data protection.

## NEGLIGENCE

Similarly, the court held that the duty of care argued for by the Claimant to establish his claim in negligence was covered by the statutory duties under the DPA. As such, there was no need to impose a duty of care in negligence and it would not be fair, just or reasonable to do so. The court followed the precedent from *Smeaton v Equifax Ltd [2013] 2 All ER 959* in which it was held that:

> "*imposing a duty owed generally to those affected by a data breach would potentially give rise to an indeterminate liability to an indetermined class…and doing so would be otiose, given the obligations imposed by the DPA".*

This lack of duty of care was fatal to the Claimant's cause of action in negligence, but the court went on to clarify that even if the Claimant had an arguable case on duty of care, he had suffered no recoverable loss. This was because there was (as yet) no evidence that his personal details had been misused as a result of the breach. While the Claimant pleaded that he had suffered distress and anxiety as a result of his personal data being accessed by the hacker and the fact that it could potentially be used to clone his identity, the court reiterated that distress/anxiety (falling short of clinically recognised psychiatric harm) is not sufficient damage to form a claim for negligence. This contrasts with actions for breach of the DPA: section 13 of the DPA makes clear that financial loss is not necessarily required and the Court of Appeal upheld in 2019 the concept of damages for mere loss of control of personal data without even any need for distress/anxiety.

## CONCLUSION

The government figures from March 2021 report that around 40% of UK businesses and around a quarter of UK charities suffered a cyber-security attack in the preceding 12 months[1]. Such events tend to have lasting regulatory and reputational effects, and data subjects themselves are increasingly motivated to take legal action, whether alone or as part of a claimant group).

This judgment is an important one for any business that suffers a cyber-attack and is concerned that it may be on the wrong end of litigation as a result. It provides certainty regarding those claims that are <u>not</u> legally arguable by affected data subjects – namely, BoC. MPI and negligence. No

doubt companies that hold large amounts of personal data will welcome this given the prospect of group litigation in these circumstances.

That does not, however, mean that businesses are off the hook entirely. Companies remain under various statutory obligations regarding data security and data subjects whose personal data is put at risk as a result of cyber-attacks may still bring claims for breach of statutory duty if it turns out that the attack was due to a failure by the company to meet those standards. Indeed, there remains an active claim against DSG for breach of DPP7, albeit that it has been stayed pending the appeal by DSG of the ICO's determination that it breached the DPA.

---

### Endnote

1. https://www.gov.uk/government/news/businesses-urged-to-act-as-two-in-five-uk-firms-experience-cyber-attacks-in-the-last-year

*The authors would like to thank Vaidehi Naik, Trainee Solicitor, for her contribution to this blog post.*

### RELATED CAPABILITIES

- Litigation & Dispute Resolution
- Business & Commercial Disputes

## MEET THE TEAM

**Oran Gelb**

Co-Author, London

oran.gelb@bclplaw.com
+44 (0) 20 3400 4168