LESSONS TO LEARN ABOUT CYBER RISKS *VARIOUS CLAIMANTS V MORRISONS SUPERMARKET PLC [2017] EWHC 3113 (QB)*

Date: 19 January 2018

UK Insurance Coverage Alert

By: Sarah Turpin, Sarah G. Emerson, Alexander J. Bradley-Sitch

A recent judgment of the High Court provides a stark lesson for organisations about the need to protect themselves properly against cyber-related risks. With the introduction of the General Data Protection Regulation ("**GDPR**") in May 2018, effective prevention and response protocols, and - vitally - comprehensive insurance coverage is a must-have for companies of all sizes.

In *Various Claimants v WM Morrisons Supermarket PLC* [2017] EWHC 3113 (QB), Langstaff J found that the defendant supermarket, Morrisons, had breached its data protection obligations and was liable to pay compensation to over five thousand current and former employees. The judge held that Morrisons, in its role as a data controller, had not breached its data protection obligations. However, an employee ("**Mr Skelton**") had breached data protection legislation (for which he is now serving an eight-year prison sentence). Morrisons was held vicariously liable for Mr Skelton's conduct.

BACKGROUND

Mr Skelton was a Senior IT Auditor, employed by Morrisons. In 2013, he had been subject to disciplinary proceedings which resulted in him receiving a formal warning. The judge in Mr Skelton's criminal trial said this formal warning caused Mr Skelton "*to harbour a very considerable grudge and harbour very considerable bad feelings towards Morrisons*". Nevertheless, Mr Skelton continued to be employed by Morrisons.

In 2014, as part of his role, Mr Skelton obtained a USB stick containing a significant amount of employee payroll data, which was intended for Morrisons' auditors. He copied the payroll data and then leaked the contents online and to newspapers. He was subsequently arrested and convicted under the Computer Misuse Act 1990 and Data Protection Act 1998 ("**DPA 1998**").

RELEVANT LAW

There are two key points of law relevant to this case:

1. First, the DPA 1998 establishes a number of rights and obligations which apply to data subjects and data controllers respectively. In particular, section 4(4) sets out the Data Protection Principles ("**DPPs**") with which data controllers are required to comply. DPP 7 provides that data controllers must take "*appropriate technical and organisational measures…against unauthorised or unlawful processing of personal data*

and against accidental loss or destruction of, and damage to, personal data." Further, it is possible for a claimant to claim 'moral' or 'distress' damages from a defendant which is in breach of its obligations, even in circumstances where actual loss has not been made out.

2. Under English employment law, an employer can be liable for the wrongful acts of its employees, if the wrongful act is sufficiently closely connected to the employee's job description. This is known as 'vicarious liability'. In this case, Mr Skelton's role as a Senior IT Auditor was held to be sufficiently closely connected to his wrongful act as to give rise to vicarious liability. The fact that Mr Skelton was acting maliciously did not enable Morrisons to escape liability for his actions.

In this case, the claimants whose data had been leaked brought a claim against Morrisons on several grounds including misuse of private information; breach of confidence; and breach of the DPA 1998 (on the basis of direct and/or vicarious liability). While the majority of the grounds for liability brought against Morrisons were dismissed, the judge found that Morrisons was vicariously liable for Mr Skelton's breach of the DPA 1998.

ANALYSIS

Various Claimants v Morrisons is significant because it highlights the risk that a data controller which is fully compliant with its obligations may nevertheless be liable for the wrongful acts of its current or former employees. The case is a classic example of a data breach caused by a disgruntled employee who has access to confidential data. It should be remembered that data breaches (as well as the consequential financial and reputational damage of such breaches) can be caused by a range of different external actors: criminals, terrorist groups, and even hostile foreign states or governments. It is not strictly necessary for a data breach to have been caused by an employee of the data controller for that controller to be held liable under data protection law.

While it remains impossible for an organisation to fully protect itself from all and any cyber risks, there are certain types of vulnerabilities that can be anticipated and minimised by undertaking a thorough cyber risk assessment. Companies should ensure they have effective security procedures and protocols in place.

Good practice aimed at prevention is essential. Equally companies should be prepared in case a breach does occur. Clear and effective response protocols should be in place. The type of compensation for which *Morrisons* was found liable as data controller, as well as the costs incurred in defending the proceedings, may be covered by insurance, if you have the appropriate cover in place. Companies should consider, as part of their risk mitigation process, what cyber-related coverage their insurance programme provides. Many traditional policy forms may not provide adequate cover and it is worth considering to what extent any potential gaps might be addressed by a dedicated cyber insurance policy.

THE FUTURE

In May 2018, the GDPR will come into force and will replace the DPA 1998. The GDPR greatly widens the potential liability of data controllers for the loss of protected data and may well lead to an increase in claims by employees, customers, business partners and others whose personal data has been compromised. This new law makes the need for companies to have effective systems in place all the more acute.

Morrisons has been granted permission to appeal the judgment. However, even if Morrisons is successful in overturning the judgment, the case serves as a stark reminder of the financial and reputational issues at stake in the event of a data breach.

If you have any questions about the contents of this alert, including the changes being introduced by the GDPR, or cyber-related insurance coverage, please contact one of the authors.

KEY CONTACTS

SARAH TURPIN
PARTNER

LONDON
+44.20.7360.8285
SARAH.TURPIN@KLGATES.COM