Ruling significantly increases organisations' exposure to data breach claims

Ian De Freitas and David Morgan| 12 December 2017

A High Court ruling has determined that Morrisons Supermarkets is vicariously liable for a data breach maliciously committed by a disgruntled employee.

The case is significant for a number of reasons:

- It is the first time that an employer has been held vicariously liable in such circumstances;
- It did not matter that Morrisons had discharged their obligations to take all necessary steps to prevent the breach;
- Data breaches committed by employees are reasonably common. Once the EU General Data Protection Regulation (GDPR) takes effect in May 2018, breaches like this will have to be reported to the affected individuals (and to the Information Commissioner). It had been thought that compliance with accepted data security standards would offer a defence to any subsequent claims by the affected individuals. This no longer appears to be the case. In effect, we have gone from a negligence standard towards one more akin to strict liability;
- It raises questions about the extent to which insurance cover for data breaches, and the consequences arising from them, is in place or available in such circumstances.

The implications of the ruling still need to play out however in two key respects:

- The High Court Judge gave permission to appeal having been troubled by the fact that the employee had engaged in a course of conduct deliberately designed to attack Morrisons' interests and the effect of this ruling was partly to visit those intended consequences on Morrisons;
- The ruling is on liability only. Compensation for the 5,518 current and former employees who participated in this group litigation is yet to be determined. The actions of Morrisons in dealing with the breach may curtail the level of such compensation. This emphasises the importance of having in place effective breach response mechanisms.

Ian De Freitas and David Morgan consider the case and its implications in more detail below.

> “Once the GDPR enters into force in May 2018, we are likely to see claims such as this increasing”

Background

The breach involved the payroll data of nearly 100,000 staff. It was committed by a senior IT internal auditor, Andrew Skelton. It included names, addresses, dates of birth, salaries, bank account details and national insurance numbers of employees. Mr Skelton published the information on a file sharing website before posting links elsewhere on the web. He also sent CD copies of the data to three newspapers (although no paper published the information). The data breach alone would not provide criminals with access to individual employees' bank accounts without further information being disclosed, although it was acknowledged that it would make the employees more vulnerable to identity theft. The Judge noted that this was a serious risk.

Morrisons found out about the breach on 13 March 2014. Within a few hours, they had taken the necessary steps to remove the material from the file sharing website. The police were alerted and, after an investigation, Andrew Skelton was arrested on 19 March 2014. Mr Skelton was sent to prison for eight years in July 2015.

Subsequently, group litigation was brought against Morrisons by 5,518 current and former employees. They claimed primary and vicarious liability for the actions of Mr Skelton in misusing their personal information. The claims were brought for breaches of the Data Protection Act (DPA), breach of confidence and misuse of private information.

Primary liability

The Judge first held that Morrisons were not primarily liable for the actions of Mr Skelton (whether for his breaches of the DPA, breach of confidence or misuse of private information). Those were his actions and not Morrisons.

The next main issue was whether Morrisons were primarily liable under the DPA for failing to take sufficient steps to prevent the breach. The DPA requires organisations to comply with a series of Principles. In this case the relevant Principle was Principle 7 which obliges organisations to take appropriate technical and organisational measures against unauthorised or unlawful processing.

The word *appropriate* is important as it implies a minimum standard that takes account of factors such as technological development, the cost of implementing security measures and the significance of the harm that may be caused from a breach.

The claimants argued that Morrisons had fallen short of Principle 7 on six issues; ranging from failing to monitor and manage Mr Skelton to not having appropriate control mechanisms in place to ensure that he had deleted the data he had access to under his role.

The Judge agreed that Morrisons had failed to discharge their duty under Principle 7 in respect of one issue: their control mechanisms to ensure data shared internally for a specific purpose is deleted once that purpose is accomplished. However, the Judge decided that this failure neither caused nor contributed to the disclosures which were made by Mr Skelton. Accordingly, Morrisons had no primary liability.

Secondary (Vicarious) liability

Vicarious liability is a concept which means that an employer can be liable for a wrongful act committed by an employee in the course of their employment, even though the employer is entirely free from blame. The critical question in this case was whether the acts of the employee were sufficiently closely connected to their employment to fix the employer with vicarious liability.

The question was considered in 2016 by the UK Supreme Court in a case[1] (also involving Morrisons) where a petrol station attendant abused a customer, ordered them to leave the premises and then physically assaulted the customer. The Supreme Court decided that the employee's duties included dealing with customers and, though his actions were a gross abuse of his position, the assault was sufficiently closely connected to his duties to fix Morrisons with liability.

The same reasoning was applied to the Morrisons' data breach. The Judge found that there was sufficient connection between Mr Skelton's position in handling, at times, large and sensitive amounts of personal data and disclosing it to others, and his later conduct in misusing it. His wrongful acts were sufficiently connected to his employment to make Morrisons vicarious liable for those acts, whether they are framed as a breach of the DPA, misuse of private information or a breach of confidence.

The Judge though remained troubled by the idea that, in finding Morrisons vicariously liable, the court was furthering the objectives of Mr Skelton in seeking to damage Morrisons. The Judge therefore granted Morrisons permission to appeal on the conclusion of vicarious liability.

Compensation

It should be remembered that this was a trial on liability only. The question of the level of compensation to each of the 5,518 claimants is yet to be determined. It is not necessary for those claimants to establish actual loss. It is enough that they have suffered distress and that the actions of Mr Skelton have interfered with their rights to control their own data. Such losses can amount to several thousand pounds per person, based on prior case law. There will be an issue about whether the actions of Morrisons in managing the breach after discovering what had happened might restrict that loss. However, there is an equally powerful argument that the deliberate (and criminal) misuse of this data might be likely to cause some of these claimants quite considerable distress.

The shape of things to come

Once the GDPR enters into force in May 2018, we are likely to see claims such as this increasing. This is because of the mandatory data breach reporting requirements in GDPR placed on data controllers, like Morrisons, to The Information Commissioner and, in sufficiently serious cases, to the affected individuals. Under current law, broadly, there are no such obligations. We are also likely to see more claims like this because GDPR encourages group litigation claims. GDPR makes provision for representative bodies to bring claims on behalf of affected individuals where there is a data breach or other breach of GDPR. We are already seeing a trend of law firms willing to act for affected groups of individuals in such cases.

[1] Mohamud v William Morrison Supermarkets plc [2016] UKSC11.

Conclusion

This decision and its implications must cause organisations to think more carefully about their liability for data breaches. Avoiding primary liability, as Morrisons did, by adopting measures which are reasonable and proportionate to the risk are of course very important. However, with insiders such as employees potentially posing what is akin to a strict liability risk, additional vigilance around employees' access rights and retention and use of data is worth re-visiting. Another priority is to check whether insurance cover is in place should rogue employees act in this way.

If you require further information on anything covered in this briefing please contact Ian De Freitas (ian.defreitas@farrer.co.uk; +44(0)203 375 7471), David Morgan (david.morgan@farrer.co.uk; +44(0)203 375 7166) or your usual contact at the firm on 020 3375 7000. Further information can also be found on the Data protection & freedom of information page on our website.