Vicarious liability and the dangerous repercussions of a rogue employee

DENTONS

December 2015

Imagine the scenario: you have a disgruntled employee who decides to leak details about your staff on to the internet. You then receive a High Court claim from your staff because of this employee's action. Can your staff really bring a claim against your business? The company did not leak the data, the employee did.

This is the situation that supermarket chain Morrisons now faces in the High Court, in what we are sure will be a hotly contested case. Andrew Skelton, a senior auditor at Morrisons, was disciplined for using the post room to send out personal packages. On March 14, 2014, Skelton (seemingly in an act of revenge) published online and sent a local newspaper personal data relating to 99,998 Morrisons staff. This information included bank account details and National Insurance numbers. Skelton was jailed for eight years in July 2015 for his actions.

On October 26, 2015, Senior Master Barbara Fontaine at the High Court (Queen's Bench Division) allowed affected staff to pursue a group claim against Morrisons. At the moment, we understand that nearly 2,000 staff are part of this action but the Senior Master has stayed the proceedings for a four-month period to allow other affected employees to join the claim.

The law

Common law provides for the doctrine of vicarious liability. This is a form of strict, secondary liability whereby persons can be liable for the acts of others even where they have not done anything wrong themselves. The relationship between an employer and an employee is necessarily capable of giving rise to vicarious liability.

The courts will then go on to consider whether the act is so closely connected with the employment that it is fair and just to make the employer vicariously liable.

The concept of the act being "closely connected" is likely to be the most contentious consideration in this case. A spokesman for Morrisons has stated that the supermarket will not accept "liability for the acts of a rogue individual" and to its knowledge no employees have suffered financial loss because of the leak of personal information. The affected employees allege that Morrisons "failed to prevent" the leak of the personal data and has exposed them to a real risk of identity theft.

Practical steps

It is important to take steps to ensure that your business is clear on its data protection obligations and the action it needs to take if that data is compromised. The sooner your business can respond to any breach, the less likely it is that your employees will suffer any loss, financial or otherwise, because of the breach.

This will likely minimise any compensation that your business will need to pay if it is found by a court to be directly, indirectly or vicariously liable for the breach.

We suggest the following:

- First, you must make sure that your business has a specific data protection policy to help it comply with its legal obligations on data protection;
- Second, consider whether any breach of your data protection policy will amount to misconduct or gross misconduct in your business (it should) and update your disciplinary policy accordingly;
- Third, establish a designated point of contact in your office for data protection to make sure someone is monitoring the business's compliance with its data protection policy/employee handbook;
- Fourth, consider whether your employees need training on data protection and more generally their confidentiality obligations whilst in the employment of the business; and
- Finally, for extraordinary occurrences, such as the leak by Skelton in this case, we suggest putting in place an emergency response plan to minimise the time that any personal data will remain in the public domain.

We will watch with interest as this claim develops. Company liability for data protection breaches is particularly topical at the moment after the Sony data hack in the United States. Sony will have to pay up to $8 million to its employees to settle the claim, which includes an amount of $3.49 million in legal fees and roughly $1,050 for each affected employee to cover the cost of credit protection services.

This article was originally published by *Complinet*.

© 2024 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. Please see dentons.com for Legal Notices.