Employees sue for compensation under the Data Protection Act

Some four thousand current and former employees of Morrisons are reportedly suing the supermarket following a high profile leak of payroll data.

The data was deliberately leaked by a former internal auditor of Morrisons who held a grudge against the supermarket following disciplinary action taken against him by the firm. The employee concerned was jailed for eight years in July for his actions.

The payroll data was posted online and was reportedly removed within 48 hours. The information included salaries, National Insurance numbers, dates of birth and bank account details. Whilst this information is not by itself enough to defraud the individuals concerned it may be in conjunction with other information. It also gives very great credibility to fraudsters posing as legitimate businesses.

It is not clear whether any of the employees concerned suffered direct financial loss as a result of the leak. The lead solicitors say that "a number of staff" were "concerned" that they had suffered financially. We understand that Morrisons immediately reassured staff that it would compensate any colleague who suffered financial loss and they maintain that they were not aware of anyone who has lost out financially.

What this is really about is compensation for distress. The Data Protection Act 1998 (the "DPA") has always included a right to claim damages, including damages for distress, for a breach of the DPA. However, following the claim of Halliday v Creation Consumer Finance Limited [2013], such claims are much easier to bring.

So how much are the employees claiming? We don't know but in Halliday the data subject concerned was awarded £750 so that's got to be a reasonable starting point. That would make £3million (plus costs) on top of the £2million that Morrisons say that they have already spent on the basis of the four thousand who have already signed up. Lead solicitors were given another four months to sign up new claimants and with up to 100,000 Morrisons employees affected, there is plenty of scope for the bill to reach £75million.

Morrisons are resisting the claims. They say that they are not accepting liability for what they describe as "the actions of a rogue

individual". Of course the DPA requires data controllers (including employers) to take "appropriate technical and organisational measures" against unauthorised processing of personal data. So it will be for Morrisons to show that they did all they reasonably could to protect the database concerned.

It is not clear exactly how the information was removed but, no doubt, solicitors acting for the employees will argue that for such a large and sensitive data set special measures should have been taken to ensure that the information could not be removed.

What can employers learn?

- Employers also need to have a strategy for dealing with significant data breaches. The initial response is critical.
- What measures are in place to protect personal data from trusted insiders? Examples include software that prevents data files from being emailed out of the organisation, disabling USB drivers and/or hosting sensitive data sets on machines isolated from the internet.
- Claimant lawyers are getting used to group litigation strategies in the UK in a way that we have not seen on this side of the Atlantic and we can expect more of the same. Large scale employers will start to take a greater interest in technical compliance with employment legislation in future years.
- Awareness of privacy rights is also growing and such claims are likely to grow in number as the law over compensation for distress develops in this area.