Your World First

CMS Law.Tax

Digital Scotland

Class actions risk puts the spotlight on cyber security investment

Americans may have long been fascinated by British culture but when it comes to legal developments it's the US which often leads while we follow. That seems to be the case with class action law suits, a long-established feature of US litigation and one that is beginning to gain traction across the UK, including Scotland, particularly following high profile data breaches.

Last year the UK saw its first successful class action arising from a mass data breach against Wm Morrisons Supermarket plc (although an appeal to the UK Supreme Court is awaited). Meanwhile, earlier this month, a class action of up to GBP 5m in damages was launched against Ticketmaster in Liverpool following a data breach from June last year.

The case against Morrisons came after a member of its IT staff stole the data, including salary and bank details, of nearly 100,000 colleagues. The employee subsequently uploaded these details onto a file sharing site and informed three newspapers of what he had done. While the individual responsible for this breach was sentenced to eight years' imprisonment, the High Court also ruled that Morrisons was vicariously liable for his actions and ordered them to pay compensation to more than 5,000 employees who were involved in bringing the case against the supermarket.

The Ticketmaster claim, involving more than 650 individuals, is the first to be issued since GDPR came into force in May last year. The claim was launched after personal and financial data of around 40,000 UK customers was stolen through malicious malware on third party software. Despite being alerted about the breach, two months passed before Ticketmaster took action. The firm pursuing the claim has stated that two thirds of its clients have suffered multiple fraudulent transactions since the breach with the remaining clients still at risk. The firm also claims that more than a third of their clients have suffered significant stress and heightened anxiety.

These cases show a growing appetite for streamlined group claims procedures in the courts which will allow individuals to more easily access remedies in cyber data breach cases. Such cases should serve as a stark 'early' warning to companies and organisations handling significant volumes of individuals' details on file of this growing area of risk.

The Morrisons case and the Ticketmaster case both involved the use of the current opt-in procedure used in the English courts which requires individual claimants to proactively opt in to a claim if they wish to be part of it. This accounts for the relatively low number of claimants as against the numbers of individuals actually affected by the breach in each case. Opt-in procedures clearly have limitations in terms of their ability to allow all affected consumers to access the benefit of any ultimate court decision that is made (or settlement agreement that is reached).

Here in Scotland a more radical US-style opt-out option for class actions is being considered, following the passing of the Civil Litigation (Expenses and Group Proceedings)(Scotland) Act 2018, legislation which makes provision for both opt-in and opt-out processes to be adopted by the Scottish courts.

The detailed rules are still to be produced, however, any opt-out class action process that is created would automatically include all Scottish based claimants who had not actively opted-out of the proceedings and would also allow in claimants from other jurisdictions on an opt-in basis. The scope of such case is therefore exponentially wider than any of the data breach claims so far brought in the English courts and considerably amplifies the potential threat. Determining the potential financial impact of such a claim would be challenging. In an era where businesses are operating under a strict GDPR regime with sizeable regulatory fines, and where cyber security breaches are a virtual inevitability, class actions arising from data breaches are a growing risk and are likely to get bigger in size and stature. The potential for Scotland to introduce an opt-out system for class actions will only heighten this threat.

It is therefore imperative for businesses to firstly be aware of the increasingly detrimental consequences of committing a data breach and take steps to minimise the chances of one occurring and its potential impact should this be unavoidable. Companies should seek advice on what proactive measures they can take to help manage and mitigate these risks and ensure they have adequate insurance in place to cover the potentially large exposures arising from class action claims.

Class action law suits have long been available to American consumers and now they are becoming more common – and more visible – here in the UK. Only through proactive planning can businesses ensure they are suitably insulated from a trans-Atlantic storm that is now hitting our shores.

This article features on *www.cyberscotlandweek.scot* in April 2019.

Contact

Graeme MacLeod
Partner
T +44 131 200 7686
E graeme.macleod@cms-cmno.com

cms.law/scotland/digital