Brian Hoffman

Partner
303.295.8043
Denver, Washington, D.C.
bnhoffman@hollandhart.com

Seventh Circuit Finds Customers' Hassles Caused by Data Breach Enough to Save a Class Action From Dismissal

Publication — 8/3/2015

When companies get hacked, they often get sued in class actions alleging deficient safeguards of customer or employee personal information. At least since 2013, courts routinely granted motions to dismiss these “data breach” lawsuits shortly after they were filed. Last week, however, the Seventh Circuit Court of Appeals issued a ruling in *Remijas v. Neiman Marcus* that may signal a change in the way courts deal with data breach lawsuits early on. This ruling adds yet another complexity as companies carefully consider their approaches to retain customers and mitigate losses after being hacked.

In its 2013 decision in *Clapper v. Amnesty International USA*, a case involving government surveillance activities, the United States Supreme Court set a high bar applicable to data breach lawsuits. The *Clapper* Court held that in order to have “standing” – the legal right to bring a “case or controversy” under Article III of the Constitution – a plaintiff's “threatened injury must be certainly impending.” The Court found that mere “allegations of possible future injury” were not sufficient.

Subsequent trial courts applying *Clapper* to data breach lawsuits generally held that if the plaintiffs' identities have not been stolen or fraudulent charges have not been charged to credit cards – in other words, if personal information has been exposed but not used – customers or employees did not have a right to sue.

Other courts distinguished *Clapper* based on the unique facts in the cases before them. For example, the 2014 *In re Adobe Sys., Inc., Privacy Litig.* case involved hackers who had gained access to the personal information of 38 million customers who downloaded Adobe software. In addressing Adobe's motion to dismiss the case, a court determined that “the risk that the Plaintiffs' data will be misused by the hackers who breached Adobe's network is immediate and very real.” Notably, the court was persuaded in part by Adobe's supposed failure to inform customers that its data protection standards allegedly were not consistent with those in the software industry. Several months later, the court in *In re Target, Corp. Data Sec. Breach Litig.* held that the plaintiffs had sufficiently alleged injuries in the form of “unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees.” In both instances, however, plaintiffs were able to articulate concrete, or “certainly impending,” injuries.

In *Neiman Marcus*, hackers gained access to the personal information of 350,000 customers. The customers sued Neiman, alleging negligence, breach of implied contract, unjust enrichment, unfair and deceptive

business practices, invasion of privacy, and violation of state data breach laws. Among other things, the customers sought damages for lost time and money they incurred resolving fraudulent charges and protecting themselves from future identity theft.

Of the customers whose personal information was exposed, only 9,200 had actually "incurred fraudulent charges" and those 9,200 were reimbursed. The trial court granted Neiman's motion to dismiss, finding that the customers failed to show injury, and thus lacked standing. The Seventh Circuit reversed the dismissal. The appellate court held that "the process of sorting things out" and the efforts taken to obtain reimbursement were sufficient injuries for their case to go forward.

As for the remaining consumers who had not incurred fraudulent charges, the court held that their efforts to mitigate any damages they may suffer in the future – for example, paying for credit monitoring services – were also sufficiently certain injuries for their case to go forward.

Yet perhaps the most surprising aspect of the *Neiman Marcus* decision is the Seventh Circuit's finding that Neiman's offer to provide free credit monitoring and identity protection services to customers constituted actual evidence that customer injuries were "certainly impending." The court explained its logic with a rhetorical question: why else would Neiman provide such services if injuries were not certainly impending?

The *Neiman Marcus* decision has received significant national attention for seeming to lower the bar for customers or employees to establish their right to sue companies who have been hacked. Ultimately, however, the reach of the decision remains to be seen. Other circuits may not follow the Seventh Circuit's reasoning. And the Neiman Marcus customers may not actually provide sufficient evidence of recoverable damages (or other elements of their claims).

In the meantime, however, the decision stands as a reminder that data breach lawsuits filed by consumers or employees are not nuisance suits that may be dispatched on a preliminary motion to dismiss. Companies should be aware that what they do to mitigate any potential harm to their customers or employees, and in turn rebuild their reputations, will be carefully scrutinized by plaintiffs' attorneys, and the court, when determining whether a threatened injury is "certainly impending."