

Seventh Circuit Resurrects Data Breach Class Action and Stymies Standing Challenge

Article By:

Joshua J. Orewiler

On July 20, 2015, the **Seventh Circuit** reinstated a data breach class action in ***Remijas v. Neiman Marcus Group, LLC***, No. 14-3122, after a 2013 *malware attack* on Neiman Marcus's computer systems that resulted in the theft of customers' credit and debit card information. The plaintiffs argued that they had constitutional standing to pursue their claims against the retailer based on an alleged increased risk of future fraudulent charges and greater susceptibility to *identity theft*. This decision is troubling and could have a potentially significant and wide-ranging impact on pending and future class actions brought in the wake of similar data breaches. In fact, plaintiffs' lawyers already are citing the decision in other data breach class actions facing Rule 12 standing challenges. See, e.g., ***In re Barnes & Noble Pin Pad Litigation***, No. 12-08617, U.S. Northern District of Illinois.

To have standing, a litigant must prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct and is likely to be redressed by a favorable judicial decision. Federal courts have dismissed similar putative data breach class actions following the U.S. Supreme Court's decision in *Clapper v. Amnesty International*, holding that plaintiffs must allege they are at imminent risk of suffering a concrete injury. In those cases, courts often have relied on the facts that (a) data breach plaintiffs had fraudulent charges reimbursed by credit card companies and (b) the defendant arranged for complimentary free credit and identity theft monitoring services.

The plaintiffs in the *Neiman Marcus* case alleged that approximately 350,000 credit and debit cards of the retailer's customers had been compromised as a result of the breach and that fraudulent charges had appeared on 9,200 of the cards. Although the plaintiffs conceded that the charges were later reimbursed or reversed, the Seventh Circuit ruled that those customers had Article III standing to bring their claims. Specifically, the court found that the plaintiffs pled sufficient allegations of harm based on their "aggravation and loss of the value of the time needed to set things straight, to reset payment associations after card numbers are changed, and to pursue relief for unauthorized charges."

In addition, the court found that the remaining plaintiffs whose cards had not been fraudulently used also had standing to pursue their claims. The court noted that the plaintiffs had alleged that the hackers deliberately targeted Neiman Marcus to obtain their credit and debit card information, and the court concluded that the plaintiffs "should not have to wait until hackers commit identity theft or credit-card fraud in order to give class standing, because there is an 'objectively reasonable

likelihood' that such an injury will occur."

The Seventh Circuit further held that mitigation expenses allegedly incurred by the plaintiffs, such as purchasing identity theft monitoring services, were sufficiently concrete injuries based on the imminent threat of future identity theft and fraudulent charges.

Turning to the second and third prerequisites for standing, causation and redressability, the Seventh Circuit rejected Neiman Marcus's argument that the plaintiffs could not demonstrate that their injuries were traceable to the breach at the retailer rather than to one of several other simultaneous large-scale breaches, including the Target breach. The Seventh Circuit ruled that where there are multiple breaches that could have compromised the plaintiffs' information, the burden shifts to the defendant to prove that its actions were not the "but-for" cause of the plaintiffs' injury.

As a result of the Seventh Circuit's decision in this case, plaintiffs may have increased success in establishing Article III standing to maintain a lawsuit following a data breach. In addition, courts (particularly in the Seventh Circuit) are likely to see an increase in the number of class action lawsuits filed as a result of data breaches. Organizations suffering data breaches now face a potentially more difficult and expensive path in defending data breach class action lawsuits.

© 2025 Vedder Price

National Law Review, Volume V, Number 205

Source URL: <https://natlawreview.com/article/seventh-circuit-resurrects-data-breach-class-action-and-stymies-standing-challenge>