

Cybersecurity, Privacy & Data Protection Alert

July 30, 2015

7th Circuit Opens Door to Data Breach Class Actions

On July 20, 2015, the U.S. Court of Appeals for the 7th Circuit issued an opinion that could dramatically change the class action landscape for companies that are victims of hackers. In *Remijas v. Neiman Marcus Gp.*, the 7th Circuit reversed the district court, ruling that Neiman Marcus (NM) customers whose credit card information was compromised had standing to bring a class action suit against the retailer.

Sometime in 2013, hackers attacked NM and stole the credit card numbers of its customers. In mid-December 2013, NM learned that approximately 350,000 cards were exposed to malware and that 9,200 of those cards were discovered to have been used fraudulently. In 2014, the plaintiffs—on behalf of the 350,000 other customers whose data may have been hacked—brought a suit for negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy and violation of multiple state data breach laws.

Upon a motion from NM, the district court dismissed for lack of standing for failure to show “injury in fact.” The plaintiffs appealed, alleging (among other injuries) that their lost time and money resolving the fraudulent charges and protecting themselves against future identity theft, and their increased risk of future identity theft, amounted to concrete, particularized injuries.

The *Remijas* court agreed that these allegations were sufficient to confer standing. With regard to the potential for future harm, the court distinguished this type of data breach from the suspected privacy incursions in *Clapper v. Amnesty Int’l USA*, 133 S.Ct. 1138 (2013). Once a breach has occurred, plaintiffs are not required to “wait for the threatened harm to materialize in order to sue”—the breach itself amounts to a substantial risk of harm.

The 7th Circuit also found that a customer’s mitigation efforts taken after a breach, such as subscribing to a credit monitoring service, qualified as a concrete injury sufficient to confer standing. It therefore reversed the district court’s dismissal and remanded.

In dicta, the opinion took a dim view of some of the plaintiffs’ other asserted injuries. It declined to give weight to the argument that plaintiffs were harmed because they spent more on NM goods than they would have had they known that NM did not take the necessary precautions to secure their data. The court also refused to create a property right for plaintiffs’ “private information,” whereby they could be harmed even if they were automatically reimbursed and there was no risk of further use of the stolen information.

Although it was not a part of the district court's decision, the *Remijas* court also ruled against NM's causation argument that the harm could have been caused by another retailer—such as Target—who was subject to similar data breaches in 2013. In such a situation, it is a company's burden to show that it is not the cause of the injury.

The 7th Circuit raised other questions for the district court to consider on remand, including the length of time that a potential victim is truly at risk of injury following a data breach. “The [Government Accountability Office] suggests at least one year, but more data may shed light on this question.” Questions of causation and damages will dominate as more data breach class actions move past the motion-to-dismiss stage.

The *Remijas* decision highlights the dynamic litigation landscape for companies after data breaches. Federal courts across the country disagree on what is sufficient harm to confer standing, but the 7th Circuit has now opened the door to viable data breach class actions premised on the fear of future harm from identity theft. Now, companies may have just as much to fear from the plaintiff lawyers as they do from the hackers themselves.

Contact Information

If you have any questions regarding this alert, please contact:

Natasha G. Kohne

nkohne@akingump.com

+971 2.406.8520

Abu Dhabi

Anthony T. Pierce

apierce@akingump.com

+1 202.887.4411

Washington, D.C.

Michelle A. Reed

mreed@akingump.com

+1 214.969.2713

Dallas

David S. Turetsky

dturetsky@akingump.com

+1 202.887.4074

Washington, D.C.

William F. Mongan

wmongan@akingump.com

+1 212.872.7452

New York