# Neiman Marcus Case Settles After Years Of Haggling Over Price Of Data Breach Cases

Posted By *Todd Rowe* On April 4, 2017 @ 9:42 am In Protecting Against the Risk,Uncategorized | No Comments

Last week, the parties in *Remijas v. Neiman Marcus*, Case No. 14-cv-1735, a class action lawsuit related to a data breach at retailer Neiman Marcus was settled in the Northern District of Illinois. The Seventh Circuit's reversal of the District Court's decision to grant Neiman Marcus' motion to dismiss was widely considered to be a favorable decision for data breach plaintiffs because it showed that plaintiffs may be able to adequately allege damages to demonstrate they had standing to bring suit. Even though we may not get to see how discovery and further motion practice may play out, the settlement provides a significant amount of guidance on the value of damages for data breach cases and the securty measures companies are expected in the short time since this breach occurred.

In 2013, the credit card information of approximately 350,000 Neiman Marcus customers was stolen by hackers. Several affected customers filed a class action against under the Class Action Fairness Act, 28 U.S.C. §1332(d). The District Court dismissed the class action suit based on its finding that the individual plaintiffs and the class member lacked standing under Article III. The Seventh Circuit found the District Court erred and held the plaintiffs satisfied Article III requirements with allegations that the Neiman Marcus data breach inflicted concrete, particularized harm on them. The Seventh Circuit was persuaded that plaintiffs suffered injury when they lost time and money resolving fraudulent charges and protecting themselves against future identity theft as well as the financial loss suffered when they bought items at Neiman Marcus that they would not have purchased had they "known of the store's careless approach to cybersecurity."

In reversing the District Court [1], the Seventh Circuit held that "[a]llegations of future harm can establish Article III standing if that harm is 'certainly impending,' but 'allegations of possible future injury are not sufficient.'" In short, the Seventh Circuit found the plaintiffs met the requirement under *Clapper* "that injury either already [has] occurred or [was] 'certainly impending.'" After the Seventh Circuit reversed the District Court's decision, the case was remanded back to the District Court for further proceedings before the parties settled the matter.

The Plaintiffs' Amended Motion for Preliminary Approval of Class Action Settlement and Certification of Settlement Class ("Motion for Preliminary Approval") filed with the District Court filed with the District Court last week indicates a Settlement Fund will be created in the amount of one million, six hundred thousand dollars $1,600,000 which will be used to pay " eligible claimants who submit valid and timely Claims." The Motion for Preliminary Approval also includes statements that this settlement will allow "Settlement Class Members and other customers shopping at Defendant's stores since this action was filed also benefit from changes to

Defendant's business practices designed to further strengthen its information technology security."

Specifically, Neiman Marcus' Memorandum filed in support of the settlement agreement states that in addition to the settlement amount, Neiman Marcus has taken the following security measures to protect customer information:

*Chief Information Security Officer*. Neiman Marcus created and filled the position of Chief Information Security Officer (CISO), an executive position with responsibility to coordinate and be responsible for Neiman Marcus's program(s) to protect the security of customers' payment card data including account numbers, expiration dates, card verification values, and cardholder names;
*Information Security Organization*. Neiman Marcus created a new organizational unit responsible for information security and has hired employees to fill the organization, including a Director of Security Operations and a Director of Security, Risk Management and Compliance;
*Senior Leadership Reporting*. Neiman Marcus increased the frequency and depth of reporting to its executive team and members of its board of directors about its cybersecurity efforts and the cybersecurity threat landscape;
*Chip-Based Payment Card Infrastructure*. Neiman Marcus equipped all of its stores with devices that allow customers to pay for purchases using payment cards containing embedded computer chips;
*Employee Education*. Neiman Marcus expanded its program to educate and train its workforce on methods to protect the privacy and security of its customers' information;
*Information Sharing*. Neiman Marcus joined several public-private partnerships that facilitate information sharing concerning cybersecurity and threat awareness.
Even though it would have been interesting to see how the parties would have handled discovery and further motion practice, this settlement is still important for the following reasons:

*First,* the small settlement amount indicates that even if plaintiffs survive a motion to dismiss and a court is willing to find allegations may give rise to the potential for damages in data breach cases, plaintiffs still may have a substantial hurdle to show they are entitled to a substantial damage award. Here, with allegations of 350,000 customers being impacted the settlement amount of $1.6 million may not provide an incentive for plaintiffs to bring these actions.

*Next,* the non-monetary portion of the settlement agreement is worthy of examination because it shows the shift in how companies approach data protection since the breach at Neiman Marcus in 2013. At the time of the breach in 2013, the fact that corporation did not have a Chief Security Information Officer and train employees on these issues may not have been surprising. Of course, a corporation that is not implementing such procedures today is operating at its own peril.

*Finally*, the Seventh Circuit's reversal of the District Court's decision granting Neiman Marcus' motion to dismiss was often cited by plaintiffs attempting to demonstrate they had standing to bring these actions. The Neiman Marcus case could have provided even more solid ground for plaintiffs if the class action plaintiffs continued their success through discovery and into trial. Of

course, it could have also shown plaintiffs' allegations may survive a motion to dismiss, but would struggle supporting those allegations as the case proceeded through discovery.

We will discuss this settlement and more at Horton Group's Anatomy Of A Cyber Attack: Risks And Threat Mitigation [2]this Thursday, April 6, 2017 at the Hilton Chicago/Oak Brook Hills Resort & Conference Center.

---



URLs in this post:

[1] In reversing the District Court: **http://privacyriskreport.com/seventh-circuit-weighs-in-on-article-iii-standing-for-data-breach-plaintiffs/**
[2] Horton Group's Anatomy Of A Cyber Attack: Risks And Threat Mitigation : **http://www.thehortongroup.com/events/anatomy-of-a-cyber-attack-risks-and-threat-mitigation-oak-brook-il?utm_source=Invite&utm_medium=Email&utm_campaign=Marketing**