

Seventh Circuit Holds That Risk of Future Fraudulent Charge on Credit Card Sufficient to Withstand Motion to Dismiss

Thursday, July 23, 2015

During the 2013 holiday season, **Neiman Marcus**, like many other retailers, discovered that its payment card systems had been compromised and customers' credit and debit card information was potentially stolen. The rush to the courthouse began, and multiple class action lawsuits were filed and later consolidated in the Northern District of Illinois under the caption **Remijas v. The Neiman Marcus Group, LLC**, Case No. 14-cv-1735. Alleged damages included, among others, unauthorized charges on credit and debit cards, the risk of future fraudulent charges and greater susceptibility to identity theft.

Neiman Marcus filed a motion to dismiss the complaint for lack of standing and failure to state a claim. The district court granted the motion to dismiss exclusively on standing grounds, holding that the injuries alleged by plaintiffs were not sufficiently concrete. The plaintiffs appealed. On July 20, 2015, the Seventh Circuit reversed, holding that the plaintiffs had shown a substantial risk of immediate harm sufficient to afford them standing to sue.

The Seventh Circuit's Rationale

Relying heavily on *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), the Seventh Circuit analyzed whether, under *Clapper*, the injury already occurred or is "certainly impending." The plaintiffs alleged that, in addition to the fraudulent charges, they spent time and money replacing cards and monitoring their credit. The plaintiffs also argued that full reimbursement for fraudulent charges is not guaranteed, and that they were at risk of future fraudulent charges and greater risk of identity theft. This, according to the plaintiffs, is sufficient to establish standing. Agreeing with the plaintiffs, the Court stated that "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." (*quoting Clapper*, 133 S. Ct. at 1147)

Interestingly, the Court considered the fact that Neiman Marcus offered credit monitoring and identity restoration services as a reason to support the plaintiffs' claim. If there were no risk of identity theft, why offer such services? "It is unlikely that they did so because the risk is so ephemeral that it can be safely disregarded." Finally, the Court's ruling appears to upend well-established law in multiple jurisdictions that costs associated with obtaining credit monitoring and identity theft protection are not sufficient to establish an injury for purposes of Article III standing.

The Court did express doubt regarding the plaintiffs' remaining allegations. Specifically, the plaintiffs alleged that they overpaid for products at "Neiman Marcus because the store failed to invest in an adequate security system," tying the failure to some form of unjust enrichment. The Court found this allegation problematic because plaintiffs are not alleging that any specific product was defective; instead, the allegation is that they were injured by shopping at Neiman Marcus. The Court also found fault with the plaintiffs' claims that they have a "concrete injury in the loss of their private information." This would mean that any person who suffered fraudulent charges would have standing even if they were automatically reimbursed, identities were not stolen, and there was no risk that they would not be reimbursed or that their information would not be used. The Court declined to support standing "on such an abstract injury."



Article By
[Cybersecurity and Data Privacy](#)
[Wilson Elser Moskowitz Edelman & Dicker LLP](#)
[Client Alert](#)
[Criminal Law / Business Crimes](#)
[Financial Institutions & Banking](#)
[Litigation / Trial Practice](#)
[7th Circuit \(incl. bankruptcy\)](#)

Analysis

The Seventh Circuit's ruling has most likely opened the floodgates for class action litigation after a data breach involving credit cards, despite the fact that most consumers will suffer little to no harm. There may be additional backlash in response to the Court's statement that if Neiman Marcus offered credit monitoring, there must be a more than ephemeral risk of later fraudulent charges and identity theft. This statement may encourage businesses that suffer a credit card breach to refrain from offering these services in the future, which has mixed consequences. On one hand, providing credit monitoring and identity restoration services to affected customers conveys goodwill and concrete results that may appease potential litigants. On the other hand, given the Court's ruling, the provision of the services might encourage potential litigants, offering them "proof" of a substantial, immediate risk.

In reality, credit monitoring and restoration services cannot monitor the compromised card on a transaction-by-transaction basis, meaning that the services do not address or prevent the risk of future fraudulent charges – the only real risk where payment card information was the only data collected. The decision to provide credit monitoring or identity restoration services will thus be a double-edged sword going forward.

Moreover, in light of what was allegedly compromised in the Neiman Marcus breach, the future risks highlighted by the Court as the basis for plaintiffs' standing are not possible. The Court discusses identity theft and the unauthorized opening of new credit cards in the class members' names. However, what was compromised here was the payment card information – the name of the cardholder, the card number, the expiration date and the security number. The information needed to open a new credit card account – mother's maiden name, a state ID and/or a social security number – was not compromised in the breach. While future fraudulent charges on the compromised cards were also considered imminent, that assumes the issuing banks did not cancel the compromised cards and provide new cards to all affected individuals once the breach was known – a standard practice that destroys the hackers' ability to use the stolen credit card information in the future.

Organizations should be advised to take proactive steps to secure their systems now. This includes implementing stronger monitoring capabilities. If an organization can catch malicious activity inside its network quickly, it can limit the number of individuals impacted and mitigate potential harm.

Aleksandra Vold assisted in researching and drafting this Alert.

© 2019 Wilson Elser

Source URL: <https://www.natlawreview.com/article/seventh-circuit-holds-risk-future-fraudulent-charge-credit-card-sufficient-to-withst>