July 27, 2015

Weil

Alert
Cybersecurity, Data Privacy & Information Management

Seventh Circuit Holds That Neiman Marcus Customers Have Constitutional Standing to Bring a Putative Class Action over a Data Breach

By Eric Hochstadt, Paul Ferrillo and Gaspard Curioni

On July 20, 2015, the Court of Appeals for the Seventh Circuit held in *Remijas v. Neiman Marcus Group, LLC*, that Neiman Marcus customers had alleged sufficient injury to have constitutional standing in their putative class action lawsuit against the luxury retailer.[1] To date, standing has been a significant hurdle facing consumers trying to bring massive putative class action lawsuits after data breaches, so this ruling and its possible spillover impact to other cases outside of the Seventh Circuit is worth following.

According to the lawsuit, a data security breach occurred between July 2013 and October 2013, when approximately 350,000 credit cards of Neiman Marcus customers were exposed to malware nested in the company's computer systems. Neiman Marcus was alerted to fraudulent charges affecting about 9,200 of its customers in December 2013, and the malware was discovered a month later. At that point, Neiman Marcus notified potentially affected customers and offered one year of free credit monitoring and identity-theft protection. Customers exposed to the cyberattack brought a putative class action on behalf of all 350,000 other consumers asserting various claims for monetary relief.[2] The named plaintiffs asserted three categories of injury for standing purposes: (i) an increased risk of future fraudulent charges and identity theft; (ii) time and money already spent to prevent future fraudulent charges and identity theft; and (iii) other harms such as overpayment for defective cybersecurity and lost control over personal information.[3]

The district court granted Neiman Marcus' motion to dismiss for lack of standing on the ground that the harm complained of was speculative and not sufficiently concrete and thus foreclosed by the Supreme Court's decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013).[4] In *Clapper*, human rights groups challenged new procedures for government electronic surveillance and alleged that their communications with individuals located abroad were at risk of being impermissibly intercepted by the government.[5] The Supreme Court held that the groups did not have standing because their claimed injury rested on the "highly speculative fear," based on a "highly attenuated chain of possibilities," that their communications would be intercepted by the government.[6] The Supreme Court reasoned that an alleged future injury can support constitutional standing only if the injury is "certainly impending," not when there is a mere possibility or even an "objectively reasonable likelihood" that the injury will come to pass.[7]

In *Remijas*, the Seventh Circuit rejected the district court's broad reading of *Clapper*. First, with regard to the claimed risk of future fraudulent charges and identity theft, the court noted that "[h]ere . . . everyone's personal data has already been stolen," whereas in *Clapper* the petitioners "only suspected" that their communications might be intercepted.[8] Also, unlike in *Clapper*, the Seventh Circuit stated there was a nonspeculative "substantial risk" that the *Remijas* plaintiffs would suffer future harm, and they "should not have to wait until hackers commit identity theft or credit-card fraud."[9]

Second, with regard to the alleged time and money already spent on measures to prevent future fraudulent charges and identity theft, the Seventh Circuit distinguished *Clapper*, where the Supreme Court made clear that parties "cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[10] In *Clapper*, the mitigation expenses were incurred, according to the Supreme Court, in the absence of "imminent" harm, and "the speculative harm [was] based on something that may not even have happened."[11] By contrast, in *Remijas*, it was uncontested that "the initial [data] breach took place."[12] According to plaintiffs, the Neiman Marcus customers had to take "immediate preventive measures" and "spend time and money replacing cards and monitoring their credit score."[13] The court found "telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection" to its customers and concluded that "[i]t is unlikely that [Neiman Marcus] did so because the risk is so ephemeral that it can safely be disregarded."[14] In these circumstances, the Seventh Circuit concluded that the alleged mitigation expenses qualified as "actual injuries."[15]

However, the Seventh Circuit found "more problematic" the third category of asserted injuries and was "dubious" that they would suffice for standing purposes.[16] The *Remijas* plaintiffs contended that they "overpaid for the products at Neiman Marcus" because they paid for but did not receive adequate cybersecurity protection for their credit card information.[17] They also contended that their private information was "an intangible commodity" and were harmed by its loss.[18] The court declined to endorse these theories and instead relied on the "plaintiffs' more concrete allegations of injury."[19] Having concluded that jurisdiction existed, the Seventh Circuit remanded the case to the district court for further proceedings.[20]

Penned by Chief Judge Wood, the panel decision in *Remijas* is a notable interpretation of the Supreme Court's decision in *Clapper* that has been a major hurdle to date in some putative class action lawsuits arising out of a data breach.[21] The Seventh Circuit's decision provides at least one view by a court of appeals of the contours of *Clapper* in circumstances where consumers allegedly suffered fraudulent charges from a data breach. Finally, the Seventh Circuit was careful to note that the allegations of injury in *Remijas* went "far beyond the complaint about a website's publication of inaccurate information, in violation of the Fair Credit Reporting Act, that is before the Supreme Court in *Spokeo, Inc. v. Robins*."[22] While *Remijas* did not present a situation where consumers were claiming injury solely from statutes allegedly being violated from a data breach, the Supreme Court may decide next Term whether or not such consumers have constitutional standing.[23]

In sum, the issue of constitutional standing in the cybersecurity and consumer protection space generally remains an area for companies to monitor carefully. A number of courts have already taken an approach to assessing standing similar to the Seventh Circuit in *Remijas*.[24] The plaintiff class action bar is now especially aware that standing is primarily a pleading issue, and thus the more substantial the breach, the more "ammunition" they have to overcoming the standing hurdle at the outset of a case.

Further, recognizing that standing is a pleading issue (and will likely be based on facts contained in the company's initial press release(s)), *Remijas* should cause companies to consider their cybersecurity posture *prior* to a breach. Do they have adequate information security policies and procedures? Have they trained their employees to be aware of the danger of spearphishing attacks? Do they have a battle-tested incident response plan? Have they

engaged with law enforcement both prior to and following the breach in full cooperation of any investigation of the incident? Answers to these questions can influence how plaintiffs draft a complaint. Finally, the *Remijas* decision may significantly impact how companies respond to data breaches, in terms of both the duration and scope of remedial measures that may be worth taking with customers, especially since those measures can affect what defenses are available to a company hit with a data breach class action lawsuit.

---

1. No. 14-3122, 2015 WL 4394814, at *1 (7th Cir. July 20, 2015).
2. *Remijas v. Neiman Marcus Grp., LLC*, No. 14 C 1735, 2014 WL 4627893, at *1 (N.D. Ill. Sept. 16, 2014).
3. *See Remijas*, 2015 WL 4394814, at *3.
4. *Id.* at *3-4 (concluding that future harm from fraudulent charges was not "concrete" because such charges would be reimbursed, and that allegations of future harm from identity theft was "a leap too far").
5. *Clapper*, 133 S. Ct. at 1142-43.
6. *Id.* at 1147-48.
7. *Id.*
8. *Remijas*, 2015 WL 4394814, at *3-4.
9. *Id.* at *4; *see also id.* at *5 ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information?").
10. *Clapper*, 133 S. Ct. at 1155.
11. *Remijas*, 2015 WL 4394814, at *5.
12. *Id.*
13. *Id.* at *4.
14. *Id.* at *5.
15. *Id.*
16. *Id.* at *6.
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.* at *8.
21. *See, e.g., Green v. eBay, Inc.*, No. 14-cv-1688, 2015 WL 2066531, at *1, *3 (E.D. La. May 14, 2015) (granting dismissal because increased risk of identity theft and fraud was not sufficient to confer constitutional standing absent misuse of hacked information); *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. 13-cv-7418, 2015 WL 1472483, at *5-6 (D.N.J. Mar. 31, 2015) (dismissing similar data breach claims for lack of standing on the basis of *Clapper* and congruent prior Third Circuit precedent).
22. *Remijas*, 2015 WL 4394814, at *3.
23. For a discussion of *Spokeo*, see David Lender, Eric Hochstadt et al., *Supreme Court to Decide Whether Plaintiffs Have Standing to Bring Class Action Lawsuits Without Proof of Actual Injury, in Class Action Monitor*, Weil 3-4 (July 2015), http://www.weil.com/~/media/files/pdfs/150393_class_action_monitor_july2015_v3.pdf.
24. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (allegations of "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees" incurred by consumers were sufficient for standing at the pleading stage); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (same: "the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real").

Cybersecurity, Data Privacy & Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy & Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein (NY)	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

Contributing Authors:

Eric Hochstadt (NY)	Bio Page	eric.hochstadt@weil.com	+1 212 310 8538
Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372
Gaspard Curioni (NY)	Bio Page	gaspard.curioni@weil.com	+1 212 310 8068