LAW.COM
An ALM Website
August 7, 2015

Neiman Marcus Ruling May Make It Easier to Establish Standing in Data Breach Cases

By Tim Miller, Sheryl Leung and Sophie Cooper

The U.S. Court of Appeals for the Seventh Circuit recently issued an important ruling regarding standing in data breach cases that could potentially have a dramatic impact on whether these cases survive motions to dismiss for lack of standing. Specifically, the ruling could make it easier for data breach class action plaintiffs to establish standing without showing actual identity theft or other misuse of their personal information.

On July 20, in *Remijas v. Neiman Marcus Group, LLC (Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015)), the Seventh Circuit reversed the district court's dismissal of the plaintiffs' putative class action complaint, holding that plaintiffs had, in fact, sufficiently established standing under Article III. The Seventh Circuit is the first federal appellate court to address the holding of the U.S. Supreme Court in *Clapper v. Amnesty Int'l USA* that the alleged injury must be "certainly impending" to be sufficiently concrete and imminent to establish Article III standing.

Background

Neiman Marcus is a high-end retail store specializing in designer apparel. At the height of the holiday shopping season in 2013, hackers installed malware on Neiman Marcus computers. The malware exposed up to 350,000 credit card numbers of Neiman Marcus customers, 9,200 of which were then used fraudulently. Neiman Marcus learned of the existence of malware on its computer systems on January 1, 2014, and disclosed the data breach nine days later. The disclosures prompted the filing of class action complaints that were then consolidated into one complaint alleging claims of negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy and violation of multiple state data breach laws.

Plaintiffs' Claims

In their suit, the plaintiffs made the types of claims that have been common in data breach cases, alleging that they suffered:

- lost time and money resolving the fraudulent charges;
- lost time and money protecting themselves against future identity theft;
- the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity; and
- lost control over the value of their personal information.
- The plaintiffs did not allege that any fraudulent charges had not been reimbursed by the credit card companies.
- The plaintiffs also alleged that they suffered two future "imminent injuries":
- an increased risk of future fraudulent charges; and
- greater susceptibility to identity theft.

The district court dismissed the class action on the grounds that the plaintiffs failed to allege sufficiently concrete and particularized injury under *Clapper*.

Seventh Circuit Ruling

The Seventh Circuit reversed the district court and remanded for further proceedings. The court noted that *Clapper* did not foreclose all future injuries as grounds for Article III standing. Instead, the court held that, where the presumed purpose of the hackers' theft of consumers' private information is to make fraudulent charges or steal consumers' identities, the plaintiffs should not be required to wait until such events occur. The court found that the plaintiffs had pled a "substantial risk of harm" from the data breach sufficient to confer class standing.

Interestingly, the court used Neiman Marcus' offer of one year of credit-monitoring services to all affected customers against the company. Though now a common practice among companies that suffer data breaches, the court used the offer as evidence that Neiman Marcus itself believed that the risk of identity theft was significant enough to warrant the costs of the credit monitoring services. Based in part on this reasoning, the court found the plaintiffs' allegations of lost value of time spent resolving fraudulent charges and costs for credit monitoring services to prevent future identity theft sufficiently "concrete" for standing.

Court Declined to Rule on Two Types of Injury

In its decision, the Seventh Circuit declined to rule on two categories of alleged injuries asserted by the plaintiffs, noting that it was "dubious" they would have sufficed for standing.

First, the court was skeptical of the plaintiffs' allegation that they never would have spent money at Neiman Marcus had they known of its alleged cybersecurity lapses, and that Neiman Marcus therefore was unjustly enriched. The court noted that prior cases recognizing similar injuries involved the purchase of defective products, an allegation absent in this case.

Second, the court declined to confer standing based on the plaintiffs' claim that they had lost control over the value of their personal information. The court noted that such a claim presupposes there is a federal property right in personal information, but that currently there is no federal law conferring such a property right.

Court Rejected Neiman Marcus' Argument on Causation and Redressability

The Seventh Circuit rejected Neiman Marcus' argument that the plaintiffs failed to allege causation and redressability. With respect to causation, Neiman Marcus had argued that the plaintiffs had not shown that their injuries were traceable to its data breach rather than to one of several other large-scale breaches that took place around the same time. The court held that the plaintiffs had pled sufficient facts to shift the burden to defendants to show which retailer was responsible.

Finally, the court rejected Neiman Marcus' arguments that the plaintiffs' injuries are not redressable by a judicial decision because they already have been reimbursed for fraudulent charges by their credit card companies. The court held that the "zero liability" feature Neiman Marcus relied upon could vary by credit card company or exclude customers who used debit cards. Accordingly, the court held that the plaintiffs alleged injury-in-fact, causation and redressability sufficient to establish Article III standing.

Where Does Remijas Fit in the Landscape of Data Breach Cases?

Remijas is the first federal appellate court decision addressing the Supreme Court's holding in *Clapper* suggesting that future injury must be "certainly impending" to satisfy Article III standing. In holding that members of the proposed Remijas class who had not suffered any actual theft or fraud had nevertheless adequately alleged standing, the Seventh Circuit sided with district courts in the Ninth Circuit that have found risk of future identify theft or fraud sufficient to confer standing even where there is no evidence of fraudulent use of that information. But, as discussed below, many district courts have found such alleged harm too speculative to establish Article III standing. Given these divergent rulings, it is worthwhile to pause and examine the landscape in the emerging area of the law.

For standing purposes, data breach cases can be viewed as falling into one or more of three categories:

- Category 1: claims of unauthorized access to a database exposing private consumer or health information to the intruder but with no evidence that the private information was copied or stolen and no evidence of misuse of such information;
- Category 2: claims of unauthorized access and exposure paired with evidence the private information was stolen, but with no evidence of any fraudulent or other misuse; and
- Category 3: claims of unauthorized access to the defendant's database plus evidence that private information was stolen combined with evidence of fraudulent use (such as fraudulent charges on a credit card).

Courts consistently hold that plaintiffs in Category 1 cases lack Article III standing. There have been a number of decisions rejecting standing in this area, including: *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (holding that plaintiffs' "allegations of an increased risk of identity theft resulting from a [data] security breach are insufficient to secure standing" where it was "not known whether the hacker read, copied, or understood the data"), and *Peters v. St. Joseph Servs. Corp.*, 74 F.

Supp. 3d 847 (S.D. Tex. 2015) (holding the breach of a health care service's network exposing employees' personal data did not constitute Article III standing absent concrete allegations of fraud or misuse). Several courts, most notably district courts in the Ninth Circuit and the Seventh Circuit in Remijas, have held that claims of potential future identity theft or fraud in Category 2 cases are sufficient to confer standing.

For example, see *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916 (holding that the "risk Plaintiff's personal data will be misused by the hackers who breached Adobe's network is immediate and very real"), and *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (holding that plaintiffs' allegations that their personal data was collected by Sony and then wrongfully disclosed was sufficient to establish Article III standing).

However, other district courts have held that Category 2-type future injury claims are too speculative to establish standing. For example, see *In re Zappos.com, Inc.*, No. 3:12-CV-00325-RCJ-VP, 2015 WL 3466943, at *7-8 (D. Nev. June 1, 2015) (threat of future harm to 24 million Zappos customers from January 2012 data breach not sufficiently immediate to confer standing where none of the 12 name plaintiffs had pled any credit card fraud or identity theft in years following breach), and *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014) (holding the theft and subsequent dissemination of personal information did not merit Article III standing).

Outside the Ninth Circuit and prior to *Remijas*, several courts rejected even Category 3-type standing claims, usually on the ground that the alleged loss (e.g., fraudulent credit card charges) had been reimbursed. For example, see *In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, No. CIV.A. 13-7418 CCC, 2015 WL 1472483 (D.N.J. Mar. 31, 2015) (holding the fraudulent filing of a plaintiff's tax return did not constitute actual injury because they had been reimbursed); and *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (finding that there was no Article III standing because plaintiffs failed to show that unauthorized charges to six out of 33 of their cards directly linked to the data breach itself). For a contrary example, see *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (holding that plaintiffs faced credible, nonspeculative risk of future harm by, in part, pointing to fraudulent charges incurred within two weeks of shopping at Michaels, noting "the chain of causation connecting a data security breach and identity theft is not so attenuated that it makes the latter risk speculative or hypothetical").

The question raised by *Remijas* is whether the Seventh Circuit's ruling will begin a shift in the courts toward more liberal standards for the pleading of Article III standing, particularly in Category 2 cases. Barnes & Noble already has argued in its data breach class action pending in the Northern District of Illinois that the Seventh Circuit's ruling does not apply to the facts of that case, arguing the Seventh Circuit's decision was influenced by the allegation that 9,200 of the 350,000 stolen credit card numbers had been used in fraudulent charges. *Remijas* likely does not apply to the Barnes & Noble class action because it is a Category 1 case; the plaintiffs in the Barnes & Noble case alleged that hackers attempted to skim credit card information from pin pads utilized in Barnes & Noble stores but have been unable to allege that class representatives' information actually was stolen.

Practice Points

Given the ubiquitous nature of the Category 2- and 3-type injuries alleged by the plaintiffs in Remijas, the Seventh Circuit's ruling may limit the ability of defendants to use the Article III standing defense in the Seventh Circuit. Whether other circuits follow suit will be watched closely by both the plaintiffs' bar and companies that handle consumer financial information.

Furthermore, although offering fraud protection following a data breach is required by law in at least Connecticut, companies that are not required to do so (i.e., because the impacted individuals are not from states requiring such protection) should more carefully evaluate whether offering such protection to customers may be seen by a court as a concession that the risk of fraud or identity theft is substantial. There is some disagreement as to whether California imposes a requirement to offer fraud protection. Some read the California law to require 12 months of identity theft protection while others read the statute to say that if identity theft protection is offered, it must be for 12 months.

Timothy A. Miller is a litigation partner in the Palo Alto office of Skadden, Arps. He focuses his practice on corporate and securities litigation, M&A litigation, shareholder derivative litigation, trade secret misappropriation, unfair business practices and unfair competition actions, as well as business tort litigation. **Sheryl S. Leung** is a litigation associate in the Palo Alto office of Skadden, Arps. She focuses her practice on white collar criminal defense, securities-related litigation and complex civil litigation. **Sophie Cooper** was a 2015 summer associate in the Palo Alto office of Skadden, Arps.