HOOSIER LITIGATION BLOG

www.PavlackLawFirm.com

July 24 **2015**

by: Colin E. Flora
Associate Civil Litigation Attorney

7th Circuit Weighs in on Crucial Standing Issue in Cyberattack Cases

Earlier this year, Anthem Blue Cross Blue Shield was target of a cyberattack that exposed information on tens of millions of its customers. Following the attack, lawyers from across the country jockeyed for position in the ensuing litigation. Knowing that it would be a case that would inevitably be subject to a multidistrict litigation panel (MDL), many firms filed suit in Indiana–the home of Anthem's corporate offices. However, to the surprise of many, when the case was pulled into the MDL, it was not assigned to an Indiana court. Instead, it was transferred to the Northern District of California to be overseen by Judge Lucy Koh. The decision to transfer the case to California, and Judge Koh in particular, stood to benefit the plaintiffs dramatically. The reason is that Judge Koh has experience in a cyberattack case and previously rejected a challenge on the grounds that most plaintiffs could not establish injury such that they possessed standing by mere virtue of having their information accessed.

Today's discussion is not about Anthem, however. The Anthem case just provides a backdrop, because at the time the Anthem case was consolidated and transferred to California, the standing issue remained an open question within the Seventh Circuit–the federal appellate circuit with jurisdiction over Illinois, Indiana, and Wisconsin. This week, that open question was answered.

The case that spurs today's discussion is *Remijas v. Neiman Marcus Grp., LLC*. It all began with a 2013 attack on Neiman Marcus that resulted in hackers

obtaining credit card numbers for around 350,000 customers. Some of these customers–around 9,200 in total–unsurprisingly, discovered fraudulent charges on their credit card accounts. As a result, some of the customers brought a putative class action case. Before the case got going, the district court dismissed the case for lack of subject matter jurisdiction. We've discussed on the Hoosier Litigation Blog the topic of subject matter jurisdiction before. However, this is a more nuanced issue of subject matter jurisdiction than our prior discussion. Instead of an issue of whether a federal court has jurisdiction over the subject of the case, the issue presented was whether the plaintiffs and the class had "standing." We have touched on the issue of a class representative's standing, but did not delve deeply into what standing is.

Standing is the product of the Constitution's requirement in Article III, section 2 that court's jurisdiction be confined to cases or controversies. From this has sprung the concept of standing. As the Seventh Circuit explained, "[i]n order to have standing, a litigant must 'prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision.'" In cyberattack cases, the difficulty is usually in proving the particularized injury. In wide-scale attacks, there are usually a great many persons whose private information has been accessed, but who have not been subject to a charge on his or her account. Specifically, the Seventh Circuit noted, "These plaintiffs must allege that the data breach inflicted concrete, particularized injury on them; that Neiman Marcus caused that injury; and that a judicial decision can provide redress for them." The district judge did not think plaintiffs could do so. The Seventh Circuit disagreed.

Writing for the unanimous panel, Chief Judge Diane Wood began the analysis by looking at the plaintiffs' proffered injuries:

> The plaintiffs point to several kinds of injury they have suffered: 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) 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 4) lost control over the value of their personal information. . . . The plaintiffs also allege that they have standing based on two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft. We address the two alleged imminent injuries first and then the four asserted actual injuries.

In addressing the issue of future harm–the "imminent injuries–the court

looked to the recent (2013) Supreme Court decision in *Clapper v. Amnesty International USA*. There, the Court held that Amnesty International failed to establish sufficiently non-speculative future injuries for federal surveillance through FISA where it could not show that the surveillance intercepted any calls between Amnesty International and a suspected terrorist. In a footnote in the *Clapper* opinion, the majority opinion recognized:

> Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.

It is on this footnote the Seventh Circuit relied. Finding that *Clapper* does not outright foreclose the use of future injuries as a basis for standing, the court looked to a persuasive district court decision that also applied *Clapper*'s recognition of the "substantial risk" approach to cyberattack cases.

What district court opinion? Why Judge Koh's opinion in *In re Adobe Systems, Inc. Privacy Litigation* of course:

> In a data breach case similar to ours, a district court persuasively applied these principles, including *Clapper*'s recognition that a substantial risk will sometimes suffice to support Article III standing. "Unlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,' the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real." *In re Adobe Sys., Inc. Privacy Litig.* Our case is much the same. The plaintiffs allege that the hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information. Whereas in *Clapper*, "there was no evidence that any of respondents' communications either had been or would be monitored," in our case there is "no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken." Like the *Adobe* plaintiffs, the 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.
>
> Requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different problem: "the

> more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach."

Concluding that at the pleading stage of the case, the plaintiffs had sufficiently shown a "substantial risk of harm" from the breach, the court added some common sense: "Why else would hackers break into a store's database and steal consumers" private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

The court then turned to the argument that plaintiffs had suffered lost time and money. The court found sufficiently concrete injury in the potential need to retain credit monitoring:

> An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for $4.95 a month for the first month, and then $19.95 per month thereafter. That easily qualifies as a concrete injury.

Although the lost time and money injury was sufficient, the court also addressed two other alleged injuries that it found more dubious, but explicitly withheld deciding. The first is that the customers overpaid for products at Neiman Marcus because the transactions did not include an implicit data security system behind the purchase. The other alleged injury was the mere access of private personal information. The former argument seems a bit of a stretch. The latter, though supported by an increased number of state statutes was still, in the court's opinion, dubious.

Having found an "injury-in-fact" the court turned its attention to the rest of the standing requirements: causation and redressability. The issue of causation sparked the court to compare the argument to a tort case that most every law student reads.

> Neiman Marcus argues that these plaintiffs cannot show that their injuries are traceable to the data incursion at the company rather than

> to one of several other large-scale breaches that took place around the same time. This argument is reminiscent of *Summers v. Tice*, in which joint liability was properly pleaded when, during a quail hunt on the open range, the plaintiff was shot, but he did not know which defendant had shot him. Under those circumstances, the Supreme Court of California held, the burden shifted to the defendants to show who was responsible. Neiman Marcus apparently rejects such a rule, but we think that this debate has no bearing on standing to sue; at most, it is a legal theory that Neiman Marcus might later raise as a defense.
>
> The fact that Target or some other store might have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are "fairly traceable" to the data breach at Neiman Marcus. If there are multiple companies that could have exposed the plaintiffs' private information to the hackers, then "the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level.

This left only the issue of redressability. Neiman Marcus argued that a judicial decision could not provide redress fraudulent charges because those charges have been reimbursed. The court recognized that the argument might be true for the 9,200 persons who suffered fraudulent charges, as there was no allegation that they were not reimbursed, but the other injuries discussed are not answered by mere reimbursement:

> Although some credit card companies offer some customers "zero liability" policies, under which the customer is not held responsible for any fraudulent charges, that practice defeats neither injury-in-fact nor redressability. The "zero liability" feature is a business practice, not a federal requirement. Under 15 U.S.C. § 1643, a consumer's liability for the unauthorized use of her credit card may not exceed $50 if she does not report the loss before the credit card is used. If she notifies the card issuer before any use, she is not responsible for any charges she did not authorize. Debit cards (used by several of the named plaintiffs) receive less protection than credit cards; the former are covered under the

> Electronic Funds Transfer Act, and the latter under the Truth in Lending Act as amended by the Fair Credit Billing Act. If a person fails to report to her bank that money has been taken from her debit card account more than 60 days after she receives the statement, there is no limit to her liability and she could lose all the money in her account. In any event, as we have noted, reimbursement policies vary. For the plaintiffs, a favorable judicial decision could redress any injuries caused by less than full reimbursement of unauthorized charges.

Thus, the Seventh Circuit found standing, at least at this juncture, for the case to proceed.

A few notes on the decision. First, this decision goes a long way toward answering the question of standing in cyberattack cases, but it does not definitively answer it. The decision is specifically confined to the procedural juncture of the case. The court goes out of its way to note that the factual development may change things. Second, am I the only one bothered by Neiman Marcus's (Marci? for my Latin scholars) argument that there is no injury to a consumer because his credit card company will bear the cost? A person injured in an automobile accident does not lose standing because the cost of his car repair and the cost of his medical bills are covered by his insurance company. True, there is pain and suffering damages that can be claimed, but so too can he recover for the property damage and the medical bills. The way this works is simply that the insurance company (or Medicare/Medicaid) retains a lien over that portion of the recovery to repay its costs. It makes no sense to me why Neiman Marcus should escape liability just because there is another industry–the credit card industry–stuck on the hook to pick up the bill for the harm of its negligence. Nevertheless, the Seventh Circuit, though not specifically answering Neiman Marcus's assertion, seemed to concede validity to the argument.

Ultimately, this is an issue that will eventually work its way to the Supreme Court for a decision. Only time will tell how the Court rules. If I were a betting man, given the importance of standing in cyberattack class action cases, I'd bet the court will rule (5-4) against standing as articulated in this case. That said, the Court will soon rule on whether congress can grant standing by authorizing a private right of action for the violation of a statutory right without need to prove injury in *Spokeo, Inc. v. Robins*. If the Court upholds the Ninth Circuit, as I expect it will, and allows congress to provide a statutory right that can be redressed without further proof of injury, then the answer to future cybersecurity cases may well be a federal law similar to Telephone Consumer Protection Act.

Join us again next time for further discussion of developments in the law.

Sources

- *Remijas v. Neiman Marcus Grp., LLC*, ---F.3d---, No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015) (Wood, C.J.).
- *Clapper v. Amnesty Int'l USA*, —— U.S. ——, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013) (Alito, J.).
- *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (Koh, J.).
- *Summers v. Tice*, 33 Cal.2d 80, 199 P.2d 1 (Cal. 1948).
- Colin E. Flora, *How Does a Class Action Case Work?*, HOOSIER LITIG. BLOG (July 6, 2012).
- Colin E. Flora, *Federal Diversity Jurisdiction and the 'Gaping Hole Problem'*, HOOSIER LITIG. BLOG (Jan. 25, 2013).
- Colin E. Flora, *Seventh Circuit Examines Standing for Class Rep and Departs from 3rd & 8th Circuits on FDCPA Interpretation*, HOOSIER LITIG. BLOG (Mar. 14, 2014).