Patterson Belknap Webb & Tyler LLP

Privacy and Data Security Alert July 2015

Remijas v. Neiman Marcus: Seventh Circuit Affords Broad Standing To Sue Over Consumer Data Breaches

When hackers breach a business's systems, class actions are sure to follow. Often, however, these suits have faltered right out of the starting gate. Citing the Supreme Court's 2013 decision in *Clapper v. Amnesty International*, many federal district judges have dismissed these suits, holding that consumers whose personal data have been compromised—but who have not actually incurred any fraudulent charges or suffered identity theft—lack standing under Article III of the U.S. Constitution.

This week, the Seventh Circuit declined to follow these decisions. This may subject businesses that collect consumer data to an elevated threat of class-action liability in Illinois, Indiana, and Wisconsin federal courts.

In *Remijas v. Neiman Marcus*, four shoppers filed a class-action complaint against Neiman Marcus over a 2013 data breach, in which "hackers" had apparently gained access to the credit card numbers of some 350,000 customers. Of those 350,000 customers, only 9,200 had actually "incurred fraudulent charges," and all of those fraudulent charges were "later reimbursed." Of the remaining customers, some had paid for credit-monitoring services or otherwise spent time or money guarding against potential fraud or identity theft, and others had not.

The Seventh Circuit held that *all* of these categories of consumers had standing to sue.

It first found that the 9,200 shoppers who had already incurred fraudulent charges had standing, even though those charges were reimbursed. This was because "there [were] identifiable costs associated with the process of sorting things out," such as the time and effort spent seeking reimbursement and updating auto-pay settings for replacement cards. Here, *Remijas* broke no new ground: courts have long held that the cost of remediating a concrete injury is itself an injury.

But what about the 97% of shoppers who had *not* experienced any fraudulent activity? As in many other cases, the district court had held that these consumers lack standing under *Clapper*. In *Clapper*, the Supreme Court found that the plaintiffs lacked standing to challenge the government's warrantless wiretapping program. It was not enough to furnish standing that *some* people in their position would inevitably be wiretapped; the question was whether *the plaintiffs themselves* would be. Because there was only a "speculative" possibility that this would occur, there was no presently existing or "certainly impending" future harm, as Article III requires.

The Seventh Circuit rejected this reasoning. It distinguished *Clapper*, observing that the *Clapper* plaintiffs "only *suspected*" that their own calls might be wiretapped, while all 350,000 Neiman Marcus shoppers *knew* that their card numbers had been "stolen." And, at least in the Seventh Circuit's view, once stolen, the likelihood that any given card number will be misused is quite high. The court cited little actual *evidence* for this proposition. Instead, it noted Neiman Marcus's voluntary offer of free credit-monitoring and identity-theft-protection services to affected shoppers, construing this as a sign that the risk of fraud was material.

Then, the Seventh Circuit went on to hold that shoppers who had not been defrauded *also* had standing to sue based on the "time and money" they had spent "protecting themselves against" the possibility of fraud. Here, too, the Court distinguished *Clapper*, which had held that plaintiffs cannot "manufacture" standing by taking preemptive measures

to avoid speculative future harm. In the data-breach scenario, the Seventh Circuit reiterated, the risk that any given consumer will eventually be defrauded is more substantial.

After *Remijas*, companies that do business in Illinois, Indiana, and Wisconsin, or serve consumers located in those states, may face an uphill battle defeating data-breach suits on standing grounds.

Companies should carefully consider whether to offer complimentary fraud protection to their customers in the event of a breach, since courts may—as the Seventh Circuit has—treat this as an indication that the risk of fraud or identity theft is substantial. Companies should also take care in how they word their public communications about data breaches, making sure not to state that personal data has *actually* been stolen, when in reality, all that is known or knowable is that data has been *exposed to the possibility* of theft. The latter scenario is much closer to the facts of *Clapper* than the scenario the Seventh Circuit believed it faced in *Remijas*.

The Supreme Court may soon clarify just how "imminent" an injury must be to impart standing in *Spokeo, Inc. v. Robins*, a privacy class action that will be argued this coming fall. Officially, the "question presented" in *Spokeo* is limited to whether a plaintiff may satisfy Article III's injury-in-fact requirement based on the defendant's "bare violation of a federal statute" (there, the Fair Credit Reporting Act). In the certiorari briefing, however, the parties squared off on whether the plaintiff's "risk of injury to [his] reputation" and "harm to his [future] employment prospects" were too "speculative" and "hypothetical" to constitute "cognizable injuries-in-fact" under *Clapper*.

Whether or not the Supreme Court reaches these issues in *Spokeo*, the Seventh Circuit's decision in *Remijas* is unlikely to be the last word.

Michael F. Buchanan	212-336-2350	mfbuchanan@pbwt.com
Michelle W. Cohen	212-336-2758	mcohen@pbwt.com
Peter C. Harvey	212-336-2810	pcharvey@pbwt.com
Jonah M. Knobler	212-336-2134	jknobler@pbwt.com
Craig A. Newman	212-336-2330	cnewman@pbwt.com
Daniel S. Ruzumna	212-336-2034	druzumna@pbwt.com
James Zucker	212-336-2653	jzucker@pbwt.com