Chicago Daily Law Bulletin®

Volume 162, No. 84 Serving Chicago's legal community for 161 years

Credit card theft plaintiffs discover warm home after 7th Circuit rulings

One of the great scourges for retail companies in the digital age has been the ever-present threat of massive data breaches by hackers attempting to steal millions of consumers' debit and credit card information.

In recent years, prominent companies as varied as Neiman Marcus, Bebe, Dairy Queen, Sourcebooks and Michaels have been targeted by cybercriminals who have sought to gain unauthorized access to customers' highly sensitive payment card data by exploiting vulnerabilities in these companies' data-security measures.

In addition to coping with the negative publicity and angry customers that inevitably accompany these breaches, companies have also been forced to defend against class actions filed by their aggrieved customers.

Many of the plaintiffs in these cases just happened to shop at a store during the discrete period of time when hackers purportedly had access to their credit card data. Thus, one of the most contested questions in data breach class actions has been the issue of whether (and under what circumstances) a consumer has standing to sue the company that inadvertently allowed the consumer's data to be compromised.

In sum, what do plaintiffs in a data breach case have to do to plausibly show that they suffered an actual injury such that they can bring a claim in federal court? Based on the recent trend in the case law, this bar is extremely low.

Last year, the 7th U.S. Circuit Court of Appeals made its first foray into this area in *Remijas v. Neiman Marcus Group LLC*, 794 F.3d 688 (7th Cir. 2015). The appeals court concluded that the plaintiffs, whose data had been compromised in a data breach targeting Neiman Marcus, had sustained injuries that were "concrete and particularized" enough to support Article III standing.

Specifically, the *Remijas* court identified two types of injuries in fact: (1) imminent "future" injuries such as the increased risks of being the victim of credit card fraud and identity theft, and (2) the time, money and anxiety plaintiffs expended in resolving fraudulent charges (even if the bank ultimately repaid them) as well as measures taken by plaintiffs to protect themselves against increased risk of identity theft or fraudulent charges.

Earlier this month, the 7th Circuit once again delved into the standing question in another data breach case and concluded that the plaintiffs' alleged injuries in this case "fit within the categories" delineated in *Remijas*.

In *Lewert v. P.F. Chang's China Bistro Inc.*, No. 14-3700 (7th Cir. Apr. 14, 2016) , the two plaintiffs had each dined at a P.F. Chang's China Bistro location in Illinois in April 2014 and used a debit card to pay for their meals.

Two months later, in June 2014, P.F. Chang's announced that its computer systems had been breached and some consumer credit and debit card data had been stolen. At the time, P.F. Chang's didn't know how many consumers were affected, whether the breach was widespread or limited to specific stores or how long the breach lasted.

By David M. Poell

David M. Poell is an associate in the Business Trial Practice Group in Sheppard, Mullin, Richter & Hampton LLC's Chicago office and focuses his practice on consumer privacy and class-action litigation. He can be reached at (312) 499.6349 or at dpoell@sheppardmullin.com.

The plaintiffs' separate cases were consolidated, and the U.S. District Court granted P.F. Chang's motion to dismiss the lawsuits for lack of subject-matter jurisdiction after concluding that the plaintiffs had not alleged a sufficient Article III injury in fact.

The dismissal came despite the fact that the alleged injuries of the two plaintiffs in *Lewert* were similar to the injuries alleged in the *Neiman Marcus* case.

One of the plaintiffs alleged that fraudulent transactions were made on his debit card so he had to cancel his card and purchased a credit-monitoring service for $106.89.

Accordingly, the 7th Circuit held that plaintiffs had alleged enough to support Article III standing and, thus, reversed the district court's ruling and remanded.

The other plaintiff did not spot any fraudulent charges, but he did allege that he spent time and effort monitoring his card statements and his credit report to ensure no fraudulent charges were made.

P.F. Chang's tried to distinguish the facts from *Remijas* by arguing that, unlike in the earlier case, P.F. Chang's contested whether the plaintiffs data was actually exposed in the breach.

The appeals court disagreed and held that this distinction (even if valid) was immaterial because the plaintiffs had plausibly alleged that their data was stolen, which was enough.

As the court noted, "when the data system for an entire corporation with locations across the country experiences a data breach and the corporation reacts as if the breach could affect all of its locations, it is certainly plausible that all of its locations were in fact affected."

Accordingly, the 7th Circuit held that plaintiffs had alleged enough to support Article III standing and, thus, reversed the district court's ruling and remanded.

The *Lewert* panel did express skepticism regarding the plaintiffs' other asserted injuries and whether they would be sufficient for standing. For example, the plaintiffs also claimed that the cost of their meals constituted an injury because they would not have dined at P.F. Chang's had they known of its poor data security.

The court also questioned the plaintiffs' claims that the "theft" of their personally identifiable data was akin to having one's car stolen and thus should support standing as well.

Although the court declined to predicate standing on these alternative grounds, the dual opinions of *Remijas* and *Lewert* have transformed the 7th Circuit into one of the more favorable jurisdictions in which to file class actions arising out of data breaches — especially breaches targeting companies with a nationwide reach.

Just a speculative risk of future credit card fraud or identity theft, without more, is apparently enough to meet the Article III standard threshold.