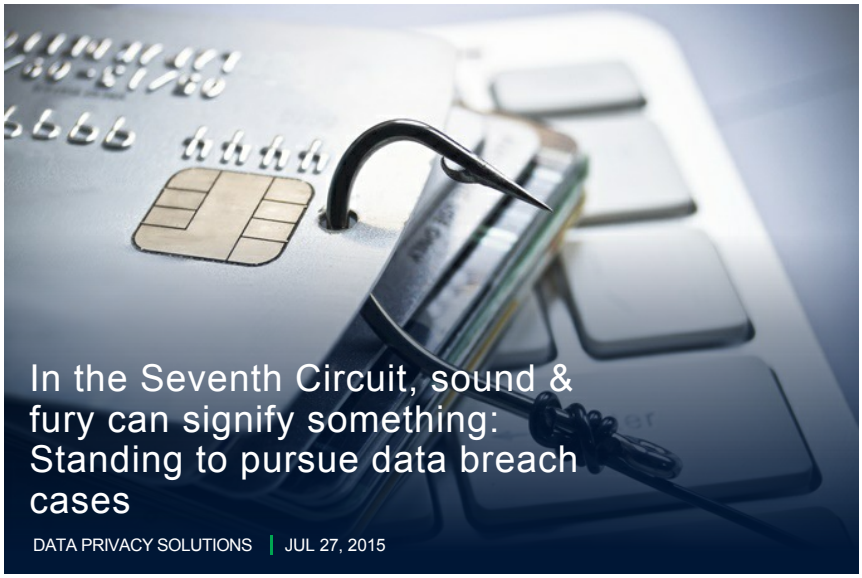

In the Seventh Circuit, sound & fury can signify something: Standing to pursue data breach cases

DATA PRIVACY SOLUTIONS | JUL 27, 2015

As the number of data breaches grows exponentially, whether an actual injury – beyond the fear and threat of future identity theft and other potential cyber harms – is required for standing continues to be a critical mass and class litigation question. In a departure from multiple decisions requiring an actual injury to create Article III standing, in *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit Court of Appeals found that, to borrow from Shakespeare's Macbeth, "sound and fury, signifying nothing" can provide standing to pursue a class action based upon a data breach.

Again, this is not the first time this issue has been addressed by courts. Courts have been on both sides with respect to what type of injury the plaintiff must assert in a data breach case to have standing – usually in cases where personal information has been compromised but the individual has not actually been harmed. On one side, the First and Third Circuits have rejected standing based on the threat of future harm as too speculative. See *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). On the other, the Seventh and Ninth Circuits allowed data breach class actions based on the threat of future harm, without any actual loss, to proceed. See *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007), and now, *Remijas et al. v. Neiman Marcus Group, LLC*, Case No. 14-3122 (7th Cir. July 20, 2015).

At issue in recent cases is the scope of the United States Supreme Court decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). In *Clapper*, human rights organizations and media groups challenged the legitimacy of the Foreign Intelligence Surveillance Act (FISA), which eased government proscriptions on obtaining wiretaps on intelligence targets outside of the United States. The plaintiffs, all U.S. citizens, asserted standing because their future communications could be intercepted. In a 5-4 decision, the Supreme Court held that the plaintiffs were unable to establish Article III standing because absent speculation, imminent injury that was "fairly traceable" to the FISA amendment could not be established. The Court acknowledged the elasticity of what "imminent" means, but were clear that the concept cannot be "stretched beyond its purpose" so an "alleged injury is not too speculative for Article III purposes."

Critically for a liability analysis in data breach cases, the Court determined that while plaintiffs' concerns were not "fanciful, paranoid, or otherwise unreasonable," the harm sought to be avoided was not "certainly impending." And standing cannot be created "merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending...If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." In *Remijas et al. v. Neiman Marcus Group, LLC* a group of Plaintiffs sued Neiman Marcus after its 2013 data breach affecting 350,000 customers' credit card information (it is estimated that 9,200 cards were used fraudulently). The company notified affected customers and offered one year of free credit monitoring and identity-theft protection. Based upon this incident, the plaintiffs' class action complaint asserted 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.

Neiman Marcus moved for dismissal on standing grounds, relying on *Clapper* and other established lines of cases, which the District Court in Northern District of Illinois (located in Chicago) granted. A unanimous panel of the Seventh Circuit Court of Appeals reversed this decision on July 20, 2015, finding that "*Clapper* does not, as the district court thought, foreclose any use whatsoever of future injuries." In the Seventh Circuit's view, *Clapper* establishes that "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 the harm." Accordingly, the Seventh Circuit determined that the Plaintiff class "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." Further, "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 … presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identity."

This decision is binding on just Seventh Circuit courts, but it will impact future cases and will be cited by scads of Plaintiffs in class and mass actions to establish standing. Moreover, it will likely embolden Plaintiffs' counsel to seek out data breach and other "no-injury" action clients.

This decision further highlights the importance of the Supreme Court's granting *certiorari* in *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S. Apr. 27, 2015). There, the critical question is whether Congress can confer standing on a plaintiff who suffers no concrete harm, but who instead alleges only a statutory violation. Again, the SCOTUS decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013) provides some insight into the direction the current Court is leaning and an extension of its prior reasoning to the *Spokeo* matter, which centers on alleged Fair Credit Reporting Act violations, is entirely appropriate. As the *Clapper* Court has established that "hypothetical future harm" is not actionable, it seems logical to conclude that a person who has not been actually injured as a result of a statutory violation cannot satisfy the injury-in-fact requirement for Article III standing. Requiring plaintiffs to plead and establish actual injury would certainly disincentivize potential plaintiffs (and perhaps, more importantly, their counsel) from filing data breach, consumer, workplace, and other class actions seeking millions in damages if they have to establish actual damages for individual plaintiffs.

Remijas v. Neiman Marcus Group, LLC should also serve as a cautionary tale for all entities, their management, and Boards. Considering the myriad of cybersecurity risks and concerns, only a comprehensive, multidisciplinary approach involving the integration of multiple legal specialties and service teams can help minimize cyber, operational, and reputational risk for companies and their governing bodies. As data breaches exponentially increase, the pool of potential plaintiffs gets bigger. Couple this with the impending increase of state and federal data breach legislation, enterprise cybersecurity must be addressed now, not (to again borrow from the Bard) "Tomorrow, and tomorrow, and tomorrow."

in the seventh circuit sound and fury can signify something standing to pursue data breach cases