CARLTON FIELDS

Contesting Standing Requirement In Data Security Suits

March 14, 2012

Law360, New York (March 14, 2012, 2:10 PM ET) -- As security breaches become more prevalent, class actions arising out of these data security breaches are now on the rise. In 2010, the Federal Trade Commission reported that there were over 725,000 cases of fraud. This is up more than 12.7 percent from 2008. Despite the increased awareness of the necessity of online security, the majority of data security breaches occur through digital contact. Large data security breaches impose significant costs on corporations to rectify the breach. For example, Sony Corp. has already had to pay an estimated $171 million to clean up the breach of the PlayStation network. *See* Larry Dignan, Sony's Data Breach Costs Likely to Scream Higher, *ZdNet*, May 24, 2011. Even aside from costs of rectifying the breach, class actions can impose additional costs on corporations, especially where plaintiffs seek hundreds of millions of dollars in damages. A recent case from the United States Court of Appeals for the Third Circuit, *Reilly v. Ceridian Corporation*, provides helpful assistance to companies litigating data security breaches. 664 F.3d 38 (3d Cir. 2011). In that case, the Third Circuit emphasizes the importance of the Article III standing requirement in data security suits and finds that allegations of possible future injury that could flow from a data security breach are not sufficient to meet the standing requirement. The findings of the Third Circuit are some of the strongest statements to date on the importance of the standing requirement in defending against data security suits. While federal appellate courts in the Seventh and Ninth Circuits have found that the standing requirement can be met by a mere threat of future harm, these cases involved an even more imminent injury than was presented in the *Reilly* case. Companies defending against data breach class actions should be aware of the subtle differences in language across the jurisdictions, but be prepared to deploy an argument requiring class action plaintiffs to show more than a mere speculative threat of future harm. The *Reilly* case involved a data security breach suffered by the Ceridian Corporation. Ceridian is a payroll processing firm that collects information about its customers' employees in order to process its commercial business customers' payrolls. Their breached data included sensitive identifying information like name, address, social security number,

date of birth and bank account information. The plaintiffs were employees of a law firm, a Ceridian customer. In December 2009, Ceridian suffered a security breach when a hacker broke into Ceridian's Powerpay system and gained access to personal and financial information belong to the plaintiffs and 27,000 employees at 1,900 companies. It was not known whether the hacker read, copied, or even understood the data. In January 2010, Ceridian sent a letter to the individuals whose personal information was at risk. The company arranged to provide affected persons one year of free credit monitoring and identity theft protection. The plaintiffs subsequently filed a lawsuit against Ceridian on behalf of themselves and other similarly situated persons. The plaintiffs alleged that they had an increased risk of identity theft, that they had incurred costs to monitor their credit activity, and that they suffered from emotional distress. The district court granted Ceridian's motion to dismiss, finding that the plaintiffs lacked Article III standing. On appeal, the Third Circuit explained that absent Article III standing, the plaintiffs claim must be dismissed. Article III to the U.S. Constitution limits the jurisdiction of federal courts to actual "cases or controversies." This is a foundational requirement that must be crossed in order for a plaintiff to have a right to sue. Allegations of hypothetical future injury are insufficient and do not establish Article III standing. Constitutional standing requires an injury-in-fact, which is an invasion of a legally protected interest that is (1) concrete and particularized and (2) actual or imminent, not conjectural or hypothetical. The Third Circuit concluded that the plaintiffs' allegations of hypothetical future injury were not sufficient to establish Article III standing. The plaintiffs speculated that the hacker: (1) read, copied and understood their personal information; (2) intends to commit a criminal act in the future; and (3) is able to use such information to the detriment of plaintiffs. The Third Circuit explained that until these conjectures come true, the plaintiffs had not suffered any injury. Because there was no misuse of information, there was no harm. Furthermore, there was no evidence to suggest that the data would ever be misused. Id. The standing inquiry is one of actuality, not one of hypothetical conjecturing. *Reilly* demonstrates the importance of the Article III standing requirement where a plaintiff in a data security lawsuit alleges a mere speculative future injury. While the Seventh and Ninth Circuits have suggested that recovery can be had for more speculative injuries, a closer examination of these cases demonstrates that the harm involved was significantly more imminent than the conjectural injury of *Reilly*. In *Pisciotta v. Old National Bancorp*, the plaintiffs argued that an increased risk of identity theft was a harm sufficient to confer standing. 499 F.3d 629 (7th Cir. 2007). In that case, the plaintiffs brought a class action against a bank after the bank's website had been hacked, claiming that the bank did not properly secure private information it solicited. While the named plaintiffs did not allege any completed direct financial loss to their accounts, the Seventh Circuit found, without much analysis, that the injury-in-fact requirement can be met by a threat of future harm. In *Krottner v. Starbucks Corp.*, the Ninth Circuit analyzed whether the plaintiffs had standing where a laptop containing the plaintiffs' personal information was stolen from Starbucks. 628 F.3d 1139 (9th Cir. 2010). The Ninth Circuit found that the plaintiffs had satisfied the standing requirement, finding that the plaintiffs had alleged a "credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." Id. at 1143. While *Pisciotta* and *Krottner* appear to allow plaintiffs to bring data security class actions when the harm is more speculative in nature, a

closer examination of these two cases demonstrates that the harm was more concrete and particularized than the harm in *Reilly*. In *Pisciotta*, there was evidence indicating that the hacker's intrusion was "sophisticated, intentional, and malicious." 499 F.3d at 632. In *Krottner*, a person tried to open a bank account with the plaintiff's stolen private information. See 628 F.3d at 1142. In contrast, the evidence in the *Reilly* case did not indicate that the hacking was malicious or that private information was used to open bank accounts. Class actions arising out of data security breaches are becoming more commonplace due to the increasing success of hackers who infiltrate complex information systems in order to retrieve personal data and financial information. Companies facing class actions alleging damage from a data security breach need to rigorously hold plaintiffs to the Article III standing requirement. Speculative future injuries are not sufficient to meet this requirement. Rather, there must be a concrete, particularized injury-in-fact. Even in those jurisdictions that use looser language on the issue of Article III standing, corporations should highlight that cases like *Pisciotta* and *Krottner* involved intentional, malicious acts and actual harm to the parties involved.