Clients&FriendsMemo

Dual Decisions Provide Narrow Path for Plaintiffs to Establish Standing in Data Breach and Cybersecurity Suits

May 23, 2016

Last week, decisions by the United States Supreme Court and the Northern District of Georgia provided further guidance regarding the narrow path required for a class action plaintiff to successfully establish Article III standing in a data breach claim brought in federal court. In *Spokeo, Inc. v. Robins*, the Supreme Court found that an online search engine's failure to accurately collect and report an individual's personal information was insufficient to establish standing, holding that a mere technical violation of a consumer protection statute without any further alleged harm to the plaintiff failed to constitute an injury that was both "concrete and particularized" and "actual or imminent."[1] Going forward, savvy defendants no doubt will argue that this standard applies to data breach and cybersecurity actions where only speculative—but not actual—economic or other harm is shown by plaintiffs. However, the Northern District of Georgia in *In re Home Depot* found that remediation costs incurred by financial institution plaintiffs as the result of a retailer's failure to secure customer information were sufficient to establish standing, even though the plaintiffs were not the ultimate victims of the breach.[2]

Together, the two decisions provide a path for certain plaintiffs to establish standing in data breach and cybersecurity lawsuits, while possibly leaving others on the courthouse steps.

I. Lack of Actual Harm May Fail the "Concreteness" Test

In *Spokeo*, the defendant, Spokeo, Inc., is an online "people search engine" that aggregates information from numerous databases and generates a profile about the subject of a search to potential employers or other third parties. In the case of the plaintiff, the profile generated by the defendant was that he was married, in his fifties, has children, holds a well-paying job, and possesses a graduate degree—all of which the plaintiff argued were incorrect and potentially could damage his future job prospects. The plaintiff initiated a class action lawsuit alleging that the defendant willfully violated the Fair Credit Reporting Act ("FCRA"), which requires consumer

---

1 *Spokeo, Inc. v. Robins*, No. 13-1339, slip op. (May 18, 2016), *available at* http://www.supremecourt.gov/opinions/15pdf/13-1339_f2q3.pdf.

2 *In re Home Depot*, No. 1-14-md-2583, 2016 U.S. Dist. LEXIS 65111 at *26-*27 (N.D. Ga. May 17, 2016).

reporting agencies to "follow reasonable procedures to assure maximum possible accuracy of" consumer reports.[3]

The District Court dismissed the complaint on standing grounds, holding that the plaintiff had not sufficiently pled an injury-in-fact as required by Article III of the United States Constitution.[4] The Court of Appeals for the Ninth Circuit reversed, finding that the plaintiff had alleged a violation of a statutory right that was protected by the FCRA, and that he had a sufficiently individualized (rather than just a collective) interest in how the defendant handled his personal information.

The Supreme Court vacated and remanded the Ninth Circuit's decision, finding that its injury-in-fact analysis failed to consider whether the plaintiff's allegations contained a sufficiently "concrete" harm. In reaching its decision, the Supreme Court noted that a concrete harm need not be tangible—an alleged intangible harm can satisfy this requirement if it has "a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." Further, the Supreme Court acknowledged—consistent with its previous holding in *Clapper v. Amnesty International USA*—that the risk of impending future harm also can satisfy the concreteness requirement under certain circumstances, including when costs are reasonably incurred to mitigate or avoid that harm.[5] However, the Supreme Court made clear that the mere allegation of a procedural statutory violation and the risk of potential future injury—without more—would be insufficient because not all such violations "entail a degree of risk sufficient to meet the concreteness requirement."[6]

II. Remediation Costs May Be Sufficient to Establish Standing

Unlike the Supreme Court in *Spokeo*, the Northern District of Georgia rejected a motion to dismiss on standing grounds in *In re Home Depot*, finding that remediation costs incurred by banks following a data breach were sufficient to provide standing.

---

[3] 15 U.S.C. §§ 1681e(b), 1681n(a). A "consumer reporting agency" is one that engages in the practice of assembling or evaluating consumer credit information for the purpose of furnishing consumer reports to third parties. 15 U.S.C. § 1681a(f).

[4] To establish standing under Article III, a plaintiff (1) must have suffered an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). To establish an injury-in-fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Id.* at 560.

[5] 133 S. Ct. 1138, 1150 n.5 (2013) (holding that standing can be "based on a 'substantial risk' that [ ] harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm").

[6] In her dissenting opinion in *Spokeo*, Justice Ginsburg argued that the concreteness requirement should be satisfied merely by establishing that a dispute between parties is "definite . . . not hypothetical or abstract," and that the plaintiff's concerns about the potential impact of Spokeo's incorrect information on his employment prospects met this requirement.

Between April and September 2014, The Home Depot, Inc. ("Home Depot") suffered a retail data breach that allowed hackers to gain access to its computer systems using the credentials of a third party vendor. Through the use of malware that was installed and went undetected for months, the hackers were able to steal the personal and financial information of approximately 56 million Home Depot customers. The stolen information then was sold on the Internet and used to make fraudulent purchases on customers' credit and debit cards.

The plaintiffs, which included a putative class of financial institutions that issued and owned payment cards compromised by the data breach, brought suit against Home Depot for negligence and negligence *per se*, as well as for violations of eight state-specific consumer protection statutes. They argued that Home Depot failed to encrypt customer data at the point-of-sale, ignored warnings from experts and its own Information Technology Department about security flaws in its system, and was deficient in properly implementing and updating antivirus software. The plaintiffs also alleged that Home Depot made it known it would not spend the money to make necessary improvements to its cybersecurity infrastructure, and even fired an employee who raised concerns about these deficiencies to management. The financial institution plaintiffs claimed they were damaged by having to reissue payment cards, investigate and refund customers for fraudulent charges, and provide customer fraud monitoring services, as well as because of interest and transaction fees lost because customers reduced their card usage. Home Depot responded by arguing that the financial institution plaintiffs lacked standing because, among other reasons, any mitigation costs they incurred, including card reissuance and fraud monitoring, were voluntary expenses that protected against hypothetical future harm, not injuries "fairly traceable" to Home Depot's alleged negligence.

The District Court found that the costs incurred by the financial institution plaintiffs neither were speculative nor were made to protect against threatened future injuries, but rather were actual and current monetary damages. In addition, the court found that any costs undertaken by the plaintiffs to avoid future harm from the data breach also qualified under *Clapper* as reasonable mitigation costs due to a substantial risk of harm. As a result, the court held that these costs were sufficiently "concrete, particularized, and actual or imminent"—and were fairly traceable to Home Depot's alleged failure to implement adequate data security measures—to establish standing for the financial institution plaintiffs to sue.

III. Conclusion

The result of the *Spokeo* decision likely will be that plaintiffs in data privacy or cybersecurity suits will lack standing unless they can show a sufficiently concrete economic harm in addition to negligence or a statutory violation. Although the Supreme Court suggested some intangible harms also may be sufficiently concrete to establish standing, it failed to provide any potential examples of what may qualify in the context of a data breach. And while the *Spokeo* Court also left open the possibility of establishing standing based on the risk of *future* harm, the only known costs that so far

appear to qualify as sufficiently concrete are those incurred to mitigate that harm. Several lower courts post-*Clapper*, however, have found that the threatened harm simply is too speculative and have denied standing even where plaintiffs have expended resources to mitigate the future harm. As a result, plaintiffs who incur monetary costs in response to data breaches of consumer information—such as the financial institutions in *In re Home Depot*—may be the last ones standing.

* * * *

If you have any questions regarding the foregoing, please contact the authors below.

Joseph V. Moreno	+1 202 862 2262 +1 212 504 6262	joseph.moreno@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com