

## CLIENT MEMORANDUM

# Supreme Court Solidifies “Concreteness” Prong of Standing Analysis for Privacy and Data Security Class Actions in *Spokeo v. Robins*

May 20, 2016

## AUTHORS

**James C. Dugan** | **Elizabeth J. Bower** | **Daniel K. Alvarez**

---

Earlier this week, the U.S. Supreme Court issued its much-anticipated decision in *Spokeo, Inc. v. Robins*.<sup>1</sup> Although the opinion left some commentators wanting more – the Court remanded to the Ninth Circuit rather than ruling on the merits – the decision offers strong guidance to lower courts evaluating standing in these oft prematurely-filed putative class actions.

Specifically, the Court reiterated, in no uncertain terms, that the injury-in-fact element of the Article III standing analysis requires a plaintiff to show that she suffered an injury that is “concrete *and* particularized and actual or imminent, not conjectural or hypothetical.” *Robins* alleged that Spokeo published inaccurate information about his background and employment status in its online database, and that an unspecified individual accessed that information. According to *Robins*, this inaccurate information resulted in lost employment opportunities, as his Spokeo profile indicated that he was overqualified for the positions to which he applied. The Court held that the Ninth Circuit, in finding that *Robins* sufficiently alleged an injury to confer standing to bring his misinformation claims under the Fair Credit Reporting Act of 1970 (“FCRA”), considered only the particularized harm prong for injury-in-fact. The Court remanded the case to the Ninth Circuit to decide whether *Robins* met the concreteness prong.

---

<sup>1</sup> *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S. May 16, 2016).

---

## Supreme Court Solidifies “Concreteness” Prong of Standing Analysis for Privacy and Data Security Class Actions in *Spokeo v. Robins*

Continued

Although the Court stated it “take[s] no position” on the ultimate outcome of Robins’s standing to bring this putative class action, the Court made three comments that indicate Robins, and putative class plaintiffs like him, have a steep hill to climb to establish a concrete harm in a typical data breach case:

1. First, the Court observed that it has “made it clear time and time again that an injury in fact must be both concrete *and* particularized.” By clarifying that the injury-in-fact requirement necessitates a two-pronged analysis, the Court has also solidified a second, perhaps more significant hurdle to establishing standing in a class action lawsuit: Even when a plaintiff establishes that harm is “personal and individual,” the plaintiff may be unable to establish that the harm is “real” or the risk of future harm is “material.” This distinct “concreteness” hurdle may be especially onerous in cases involving intangible harm.
2. Second, the Court emphasized that satisfaction of the concreteness requirement involves demonstrating “*real* harm.” Although the Court recognized that “intangible injuries can nevertheless be concrete,” it held that alleging a “bare procedural violation,” without further injury, does not satisfy Article III because violations of procedural rights do not necessarily result in actual harm. This undoubtedly will have implications for future cases brought under FCRA, as well as the Telephone Consumer Protection Act (TCPA), the Fair and Accurate Credit Transactions Act (FACTA), and the Biometric Information Privacy Act (BIPA), as all of these statutes allow plaintiffs to file claims concerning technical statutory violations even in the absence of harm. In the data breach context, there are also numerous rights granted that are arguably procedural—from breach notification to security measures—and the determination that violations of these alone, without additional harm, do not confer standing means many potential plaintiffs will fail to establish the requisite “real” harm.
3. Third, the Court provided some preliminary guidance on when a *risk* of real harm is sufficiently concrete to establish standing by emphasizing the requirement that there be a “*material risk* of harm.” This emphasis on a “material risk” of harm strikes at the center of an ongoing debate among the circuit courts about harm in the data-breach context since *Clapper* announced that a threatened injury must be “*certainly impending*” to constitute injury in fact.<sup>2</sup> While courts have generally agreed that allegations of actual financial harm and actual identity theft are sufficiently concrete harms to establish standing, courts have disagreed on whether to grant standing on the basis of an increased risk of *future* financial harm and identity theft. Purporting to apply *Clapper*, the Seventh Circuit in *Remijas v. Neiman Marcus* granted standing to all 350,000 plaintiffs who had their credit card information stolen, despite only 9,200 experiencing fraudulent charges, finding an “objectively reasonable likelihood” that an injury would occur to the remaining plaintiffs.<sup>3</sup> This relaxed approach to the risk of future injury was recently rejected by the district court in *Alonso v. Blue Sky Resorts*, which noted even before *Spokeo* that

---

<sup>2</sup> *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013).

<sup>3</sup> *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

---

## Supreme Court Solidifies “Concreteness” Prong of Standing Analysis for Privacy and Data Security Class Actions in *Spokeo v. Robins*

Continued

“such a standard is at odds with binding Supreme Court precedent governing standing,”<sup>4</sup> and appears to be in danger after *Spokeo*. An appeal was filed in *Alonso* on the same day *Spokeo* was announced, and thus will likely present the first true test of *Spokeo*'s new standard for “material risk” of harm as applied in the data breach context.

The Court's decision in *Spokeo* will likely have a direct impact on the viability of future privacy and data security class action lawsuits, particularly where a key allegation in the class action is based on the defendant's violation of a procedural right granted by statute, such as breach notification provisions. Further, while plaintiffs in class action lawsuits may allege with particularity the harm suffered, the Court's emphasis on demonstrating a “concrete” injury may prove a bar to class certification under Rule 23(b)(3)'s predominance requirement due to the difficulty of establishing class-wide concrete injury while maintaining sufficient particularity.

While *Spokeo*'s most obvious application is to consumer class action lawsuits, principles concerning injury-in-fact may be easily imported into government enforcement actions. The potential spillover effects for data security regulators and enforcers in particular make this decision interesting, especially in light of the parallels between the fact pattern and legal theories in *Spokeo* and many of the consumer protection actions by agencies such as the Federal Trade Commission (“FTC”).

The FTC is already embroiled in a pitched battle over the role of “harm” in its enforcement of data security norms under Section 5 of the FTC Act. In November 2015, an FTC Administrative Law Judge (“ALJ”) dismissed a complaint against LabMD for failure to show that the alleged unreasonable security practice “caused, or is likely to cause, substantial injury to consumers,” as required by Section 5(n)—despite the fact that the breach exposed the medical billing information for over 9,000 consumers to a peer-to-peer file-sharing network.<sup>5</sup> The FTC continues to argue in its administrative appeal that it need not prove actual harm, but rather that “[t]he actual harm is the *significant risk of concrete harm* caused by the data security practices.”<sup>6</sup> *Spokeo* may not be directly applicable to the FTC's enforcement of Section 5, but the ALJ's rejection of the FTC's argument about harm in *LabMD* combined with the Supreme Court's emphasis of “concreteness” in *Spokeo* appear to signal that the FTC and other data security enforcers will face significant barriers pursuing data-security-related violations in the future.

The impact of *Spokeo* on data breach and security cases should be carefully monitored as courts and enforcement agencies adapt to the clearer, stricter approach to Article III standing.

---

<sup>4</sup> *Alonso v. Blue Sky Resorts, LLC*, 2016 WL 1535890, at \*5 (S.D. Ind. Apr. 14, 2016).

<sup>5</sup> 15 U.S.C. § 45(n) (2016); see generally Initial Decision, In re LabMD, Docket No. 9357 (F.T.C. Nov. 13, 2015), available [here](#).

<sup>6</sup> Transcript of Oral Argument at 7, In re LabMD, Inc., Docket No. 9357, (F.T.C. Mar. 8, 2016), available [here](#) (emphasis added).

.....

**Supreme Court Solidifies “Concreteness” Prong of Standing Analysis for Privacy and Data Security Class Actions in *Spokeo v. Robins***

Continued

---

If you have any questions regarding this memorandum, please contact James C. Dugan (212-728-8654; jdugan@willkie.com), Elizabeth J. Bower (202-303-1252; ebower@willkie.com), Daniel K. Alvarez (202-303-1125; dalvarez@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at [www.willkie.com](http://www.willkie.com).

May 20, 2016

Copyright © 2016 Willkie Farr & Gallagher LLP.

This memorandum is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum may be considered advertising under applicable state laws.