ORAL ARGUMENT SCHEDULED FOR MARCH 31, 2017

No. 16–7108

United States Court of Appeals for the D.C. Circuit

CHANTAL ATTIAS, Individually and on behalf of all others similarly situated, *et al.*,

Appellants,

v.

CAREFIRST, INC., *et al.*,

Appellees.

BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS *AMICUS CURIAE* IN SUPPORT OF APPELLEES

On Appeal from the U.S. District Court
for the District of Columbia, No. 1:15-cv-882 (CRC)
Hon. Christopher R. Cooper

Kate Comerford Todd
Steven P. Lehotsky
Warren Postman
U.S. CHAMBER LITIGATION CENTER
1615 H Street, N.W.
Washington, DC 20062
(202) 463-5337

Andrew J. Pincus
Archis A. Parasharami
Stephen C.N. Lilley
Daniel E. Jones
MAYER BROWN LLP
1999 K Street, N.W.
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Attorneys for Amicus Curiae
The Chamber of Commerce of the United States of America

CERTIFICATE OF PARTIES, RULINGS, AND RELATED CASES PURSUANT TO CIRCUIT RULE 28(a)(1)

A. Parties and Amici. All parties, intervenors, and other *amici* appearing in this Court are listed in the Brief for Appellees.

B. Rulings Under Review. An accurate reference to the rulings at issue appears in the Corrected Brief for Appellants.

C. Related Cases. An accurate statement regarding related cases appears in the Brief for Appellees.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure and D.C. Circuit Rule 26.1, *amicus curiae* The Chamber of Commerce of the United States of America hereby submits the following corporate disclosure statement:

The Chamber of Commerce of the United States of America ("Chamber") states that it is a non-profit, tax-exempt organization incorporated in the District of Columbia. The Chamber has no parent corporation, and no publicly held company has 10% or greater ownership in the Chamber.

STATEMENT REGARDING CONSENT TO FILE AND SEPARATE BRIEFING

All parties have consented to the filing of this brief.† The Chamber filed its notice of intent to participate in this case as *amicus curiae* on February 15, 2017.

Pursuant to Circuit Rule 29(d), the Chamber certifies that a separate brief is necessary to provide the perspective of the Chamber, and the businesses that it represents, regarding the importance of the Article III standing issue presented by this case.

† No counsel for a party authored this brief in whole or in part, and no person other than the *amicus curiae*, its members, or its counsel contributed money that was intended to fund the preparation or submission of this brief. *See* Fed. R. App. P. 29(c)(5).

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES[1]

Page(s)

CASES

[1] Authorities upon which we chiefly rely are marked with asterisks.

RULES

OTHER AUTHORITIES

INTEREST OF THE AMICUS CURIAE

The Chamber of Commerce of the United States of America is the world's largest business federation. It represents 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country.

An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases that raise issues of concern to the nation's business community. The Chamber participated as an *amicus* before the Supreme Court at both the petition and merits stages in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

The Chamber has a significant interest in the Article III standing issue presented by this case because its members frequently face putative class action lawsuits alleging claims arising from data breaches—including allegations of bare statutory violations—without any assertion that the plaintiff has suffered actual harm. The Supreme Court in *Spokeo* affirmed that the Constitution requires plaintiffs to

allege concrete, *i.e.*, "real," harm—rejecting the contention that alleging a bare statutory violation automatically satisfies Article III's injury-in-fact requirement. And the Court also pointed to its prior holding in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), that a "risk of real harm" in the future suffices only if the future harm is "certainly impending" rather than merely possible. *Id.* at 1143.

If, despite the mandates of *Spokeo* and *Clapper*, plaintiffs are permitted to pursue cases like this one, the Chamber's members will be mired in lawsuits over breaches that have not caused any actual or imminent harm to the plaintiffs—and yet those cases threaten to extract massive settlements from businesses that were victimized by hackers or thieves. The Chamber therefore urges faithful adherence to Article III's standing requirements, which ensure that the federal courts are open to lawsuits addressing real harms but closed to lawsuits that are designed to force costly settlements rather than redress actual harms.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case is a prime example of the type of no-injury lawsuit that the Supreme Court held in *Spokeo* cannot proceed in federal court. The district court correctly dismissed the suit for lack of standing, concluding that five of the seven named plaintiffs failed to allege injury-in-fact because "merely having one's personal information stolen in a data breach is insufficient to establish standing" unless the plaintiff plausibly alleges that there is "a substantial risk that stolen data has been or will be misused in a harmful manner." Dist. Ct. Op. 2.[1]

Plaintiffs and their *amici* principally resist this conclusion on two grounds. *First*, they assert that it is enough simply to allege that CareFirst violated a statute—here, the District of Columbia's consumer protection laws. Pls. Br. 10-14; EPIC Br. 7-15, 22-23. But that is the precise theory that had been adopted by the Ninth Circuit and then *rejected* by the Supreme Court in *Spokeo*. Specifically, the Supreme

[1] The court held that the remaining two plaintiffs, who alleged that they were the victims of tax-refund fraud, had failed to establish the causation requirement of Article III standing by plausibly asserting that their alleged injury was "fairly traceable to the challenged action." *Clapper*, 133 S. Ct. at 1147. CareFirst's brief explains in detail why the district court's conclusion on that score is correct (CareFirst Br. 19-23); the Chamber focuses here on Article III's injury-in-fact requirement.

Court held that the allegation of a bare statutory violation is not sufficient by itself to confer standing—as this Court has already recognized in *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511 (D.C. Cir. 2016). Article III requires more: an injury to "some 'concrete interest' that is '*de facto*,' 'real,' and 'actually exist[s].'" *Id.* at 514 (citing *Spokeo*, 136 S. Ct. at 1548, 1549).

Second, relying primarily on cases from the Sixth and Seventh Circuits, plaintiffs and their *amici* urge the Court to relax the standard for what counts as a "risk of future harm" articulated by the Supreme Court in *Clapper* and *Spokeo* and instead hold that mere exposure to a data breach automatically satisfies Article III. *E.g.*, Pls. Br. 16-20; NCL Br. 10-13. But the cases on which plaintiffs rely are readily distinguishable and do not support this categorical approach. Moreover, the policy grounds advanced by their *amici* for such a rule cannot overcome the constitutional requirements of Article III as interpreted by the Supreme Court; and those policy arguments are in any event misguided.

Notably, the Fourth Circuit recently rejected a similar invitation to loosen Article III's injury-in-fact requirement in another data breach

case: "*Clapper*'s discussion of when a threatened injury constitutes an Article III injury-in-fact is controlling here." *Beck v. McDonald*, --- F.3d ----, 2017 WL 477781, at *6 (4th Cir. Feb. 6, 2017).

Applying these standards, the district court was correct in dismissing the claims of five of the named plaintiffs, because the harms those plaintiffs have asserted do not pass muster under *Spokeo* and *Clapper*. The judgment of the district court should be affirmed.

ARGUMENT

I. *Spokeo* And *Clapper* Govern The Article III Standing Inquiry In This Case.

The "'irreducible constitutional minimum'" of Article III standing is that "[t]he plaintiff must have (1) 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." *Spokeo*, 136 S. Ct. at 1547 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). To establish Article III standing, a plaintiff therefore must "'[f]irst and foremost'" demonstrate that she suffered "an injury in fact" that is both "concrete and particularized." *Spokeo*, 136 S. Ct. at 1547-48 (quoting *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 103 (1998)); *see also Hancock*, 830 F.3d at 513. In the context of this case,

that means that plaintiffs must allege a "concrete injury in fact stemming from the alleged violations of D.C. law." *Hancock*, 830 F.3d at 515. The attempts by plaintiffs and their *amici* to avoid that requirement run headlong into Supreme Court precedent.

A. *Spokeo* Holds That Alleging A Bare Statutory Violation "Divorced From Concrete Harm" Cannot Satisfy Article III.

Plaintiffs and their *amici* first contend that simply alleging a violation of District of Columbia law is by itself sufficient to establish standing. EPIC, for instance, repeatedly insists that an injury in *law*, rather than in *fact*, is all that Article III requires. *E.g.,* EPIC Br. 4, 7-15, 26. But that was the legal rule adopted by the Ninth Circuit in *Spokeo*, *see Robins v. Spokeo, Inc.*, 742 F.3d 409, 413 (9th Cir. 2014), and squarely rejected by the Supreme Court, which held that a plaintiff cannot plead a concrete "injury in fact" merely by alleging a bare statutory violation "divorced from any concrete harm." *Spokeo*, 136 S. Ct. at 1549. Instead, the Court stated, "Article III standing requires a concrete injury *even in the context of a statutory violation*." *Id.* (emphasis added).

In the context of the D.C. Consumer Protection Procedures Act—one of the statutes at issue here—this Court has held that *Spokeo* confirms that "the legislature 'cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing' under Article III." *Hancock*, 830 F.3d at 514 (quoting *Spokeo*, 136 S. Ct. at 1547-48). "Instead, an asserted injury to even a statutorily conferred right 'must actually exist,' and must have 'affect[ed] the plaintiff in a personal and individual way.'" *Id.* (citations omitted).

Numerous other circuits have also recognized that the Supreme Court meant what it said in *Spokeo*—plaintiffs may not satisfy their obligation to establish standing by asserting only "the invasion of a legal right that Congress created." *Braitberg v. Charter Comm'cns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (emphasis and quotation marks omitted); *see also Nicklaw v. CitiMortgage, Inc.*, 839 F.3d 998 (11th Cir. 2016) ("Article III is not satisfied every time a statute creates a legal obligation and grants a private right of action for its violation."); *Lee v. Verizon Commc'ns, Inc.*, 837 F.3d 523, 529 (5th Cir. 2016) ("*Spokeo* recognize[d] that at minimum, a 'concrete' intangible injury based on a

statutory violation must constitute a 'risk of real harm' to the plaintiff.").

Although plaintiffs rely on certain decisions by the Sixth and Seventh Circuits, those courts have nonetheless rejected plaintiffs' interpretation of *Spokeo*. In *Meyers v. Nicolet Restaurant of De Pere, LLC*, 843 F.3d 724, 727 (7th Cir. 2016), the Seventh Circuit explained that, under *Spokeo*, the legislature "does not have the final word on whether a plaintiff has alleged sufficient injury for purposes of standing." Even when a legislature "has passed a statute coupled with a private right of action," "the plaintiff still must allege a concrete injury that resulted from the violation *in his case*." *Id.* (emphasis added). Simply put, "one of the lessons of *Spokeo*" is that "[a] violation of a statute that causes no harm does not trigger a federal case." *Id.* at 727 n.2. That is true regardless of whether the statutory "right is characterized as substantive or procedural"; in either case, "its violation must be accompanied by an injury-in-fact." *Id.*

And the Seventh Circuit has underscored this point more recently in a case involving personally identifiable information, holding that standing turns on whether the plaintiff alleges a concrete injury in fact,

rather than whether he alleges a statutory violation. *Gubala v. Time Warner Cable, Inc.*, --- F.3d ----, 2017 WL 243343, at *3 (7th Cir. Jan. 20, 2017). Specifically, the court held, a plaintiff must plausibly allege a "risk of harm to himself from" the statutory violation that is "substantial enough to be deemed 'concrete.'" *Id.* at *2 (citing *Spokeo*, 136 S. Ct. at 1549). If the rule were otherwise, "the federal courts would be flooded with cases based not on proof of harm but on an implausible and at worst trivial risk of harm." *Id.*

The Sixth Circuit too has rejected the argument that, under *Spokeo*, "merely alleging a violation of ERISA rights" is enough to "satisfy [plaintiffs'] obligation under Article III." *Soehnlen v. Fleet Owners Ins. Fund*, 844 F.3d 576, 582 (6th Cir. 2016). Rather, a claimed "'concrete' intangible injury based on a statutory violation must constitute a 'risk of real harm' to the plaintiff." *Id* (quoting *Spokeo*, 136 S. Ct. at 1548).

Without so much as acknowledging the decisions just discussed, plaintiffs and their *amici* nonetheless insist that *Spokeo* applies only to "procedural" violations. *See, e.g.*, Pls. Br, 12; EPIC Br. 9-12. That argument misunderstands *Spokeo*. The Supreme Court did cite a "bare

procedural violation" as an "*example*" of a violation that, in the absence of concrete harm, would not satisfy the injury-in-fact requirement. 136 S. Ct. at 1549 (emphasis added). But the concrete-harm requirement is *not* limited to "procedural" violations. The Court held that "Article III standing requires a concrete injury even in the context of a statutory violation" (*id.*)—and that holding applies to a statutory violation of *any* kind, procedural or otherwise. After all, "'Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.'" *Id.* at 1547-48 (quoting *Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997)); *see also Hancock*, 830 F.3d at 514; *Gubala*, 2017 WL 243343, at *3.

In short, *Spokeo* confirms, as the Supreme Court has repeatedly made clear, that the injury-in-fact requirement requires that the plaintiff allege *real-world adverse consequences* from an alleged statutory violation; simply pleading a statutory violation without an accompanying concrete injury does not satisfy Article III.

B. Under *Clapper*, Potential Future Harm Either Must Be "Certainly Impending" Or There Must Be A "Substantial Risk" That The Harm Will Occur.

Although they purport to be applying *Clapper*, plaintiffs urge this Court to adopt a categorical rule that the theft of personal information in a data breach *automatically* creates a risk of future harm that satisfies Article III. *E.g.*, Pls. Br. 20 ("The Named Plaintiffs have had their data stolen by data thieves, as defined by CareFirst. Therefore, there is a substantial risk of future harm that rises above the threshold to find injury-in-fact."). This *per se* approach to standing in data breach cases squarely conflicts with *Clapper*, which supplies the governing standards.

In *Clapper*, the Supreme Court reiterated its "well-established requirement that threatened injury must be 'certainly impending'" to establish Article III standing. 133 S. Ct. at 1143 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)); *see also Lujan*, 504 U.S. at 564 n.2. Accordingly, "'[a]llegations of *possible* future injury' are not sufficient," which is why the Court rejected the Second Circuit's proposed lesser standard, which would have required only an "objectively reasonable likelihood" of future harm. *Clapper*, 133 S. Ct. at 1147 (quoting

Whitmore, 495 U.S. at 158). *Clapper* further instructs that allegations of future harm cannot "rest on speculation about the decisions of independent actors" who are not before the Court or on a "speculative chain of possibilities." *Id.* at 1150.

Clapper noted that, in prior cases, plaintiffs had not been required to plead that it was "literally certain that the harms they identify will come about." 133 S. Ct. at 1150 n.5. Those decisions found standing when there was a "substantial risk" of harm sufficiently certain to make "reasonable" the expenditure of "costs to mitigate or avoid that harm." *Id.* But the Supreme Court expressed doubt over any distinction between the "certainly impending" standard and the "substantial risk" standard. *Id.* It held that an "attenuated chain of inferences necessary to find harm" cannot satisfy either test—"to the extent the 'substantial risk' standard is . . . distinct from the 'clearly impending' requirement" at all. *Id.*; *see also Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) ("An allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.") (citing *Clapper*, 133 S. Ct. at 1150 n.5).

Clapper further held that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 133 S. Ct. at 1151. To hold otherwise would "improperly water[] down the fundamental requirements of Article III" and allow "an enterprising plaintiff . . . to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.*

While *Clapper* involved a challenge to alleged government surveillance, the Supreme Court's articulation of Article III's requirements was not limited to *Clapper*'s specific circumstances. The Court in *Spokeo* made that abundantly clear, pointing to its decision in *Clapper* to explain that the "risk of real harm" in the future may "satisfy the requirement of concreteness." *Spokeo*, 136 S. Ct. at 1548 (citing *Clapper*, 133 S. Ct. 1138); *see also id.* at 1550 (explaining that plaintiffs must allege a "material risk of harm"—*i.e.,* "a degree of risk sufficient to meet the concreteness requirement"). Thus, the inquiry

into standing must be undertaken "with *Clapper*'s tenets firmly in tow." *Beck*, 2017 WL 477781, at *7.[2]

C. Plaintiffs' Attempts To Allege Concrete Injury Do Not Satisfy Article III.

Plaintiffs' allegations of harm fall far short of what *Spokeo* and *Clapper* require. Plaintiffs cannot satisfy Article III based on their (1) fear of future identity theft; (2) self-incurred expenses based on that fear; or (3) bare assertion of an invasion of privacy.

1. Plaintiffs' allegation of an increased risk of identity theft boils down to an assertion that any data breach involving personal information automatically satisfies Article III. Yet here, there are no allegations plausibly asserting any actual misuse of the plaintiffs' (or anyone's) data as a result of the breach, or even that the type of data stolen—here, names, birthdates, email addresses, and subscriber identification numbers—could place plaintiffs at substantial risk of identity theft in the future.

[2] The Fourth Circuit in *Beck* determined that it was not required to interpret *Spokeo*, because, unlike the plaintiffs here, the plaintiffs before the Fourth Circuit did not allege that a statutory violation "alone constitute[s] an Article III injury-in-fact." 2017 WL 477781, at *5 n.4.

As CareFirst has persuasively explained, these circumstances are dramatically different from the Sixth and Seventh Circuit cases on which plaintiffs rely. CareFirst Br. 13-16 (discussing *Galaria v. Nationwide Mut. Ins. Co.*, --- F. App'x ----, 2016 WL 4728027 (6th Cir. Sept. 12, 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); and *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688 (7th Cir. 2015)). The district court in this case—as well as two other federal district courts, including one in the Seventh Circuit—correctly concluded that it is entirely consistent with *Remijas* and *Lewert* to hold that there is no standing under the circumstances presented by *this* data breach. *See Chambliss v. CareFirst, Inc.*, 189 F. Supp. 3d 564, 571 (D. Md. 2016); *Unchageri v. CareFirst of Md., Inc.*, 2016 WL 8255012 (C.D. Ill. Aug. 23, 2016), *reconsideration denied*, 2016 WL 8255013 (C.D. Ill. Nov. 4, 2016).

The speculative nature of plaintiffs' fear of future identity theft is made all the more apparent by the staleness of the breach. The breach took place in June 2014, over two-and-a-half years ago. And "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Beck*, 2017 WL 477781, at *8

(quoting *Chambliss,* 189 F. Supp. 3d at 570); *see also, e.g.*, *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958 (D. Nev. 2015) ("[T]he passage of time without a single report from Plaintiffs that they in fact suffered the harm they fear must mean something.").

Plaintiffs make much of the court's question in *Remijas*, asking "[w]hy else would hackers breach into a store's data base and steal consumers' private information" other than to commit identity theft? Pls. Br. 17 (quoting *Remijas*, 794 F.3d at 693). But that is the wrong question: If plaintiffs invoke that language to assert that Article III standing turns on the subjective intentions of unknown third parties, rather than the actual risk plaintiffs face as a result of the particular breach at issue, *Clapper* squarely forecloses that approach.

The Court in *Clapper* "decline[d] to abandon [its] usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors" like the unknown hackers who may or may not decide, or even be able, to misuse plaintiffs' information. 133 S. Ct. at 1150. The injury that plaintiffs assert here is merely theoretically *possible*, rather than "certainly impending." *Id.* at 1148.

Accordingly, the district court correctly held that the allegation that the data breach was committed by criminal hackers does not remove the "series of assumptions required to find concrete harm" in this case, including, "at a minimum, that the hackers have the ability to read and understand Plaintiffs' personal information, the intent to 'commit future criminal acts by misusing the information,' and the ability to 'use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs'] names.'" Dist. Ct. Op. 7-8 (quoting *Chambliss*, 2016 WL 3055299, at *4 (quoting in turn *In re SuperValu, Inc. Customer Data Sec. Breach Litig.*, 2016 WL 81792, at *5 (D. Minn. Jan. 7, 2016))).

The district court further correctly recognized that *Clapper* precludes reliance on such speculative harms. This "highly attenuated chain of possibilities" hypothesized by plaintiffs "does not satisfy the requirement that threatened injury must be certainly impending." *Clapper*, 133 S. Ct. at 1148.

2. Plaintiffs' credit monitoring expenditures based on anxiety about identity theft are inadequate for the same reasons that the plaintiffs' expenditures based on "subjective fear of surveillance" were

deemed too speculative in *Clapper*. 133 S. Ct. at 1153. Indeed, the Supreme Court in *Clapper* squarely rejected the theory that plaintiffs can "establish standing by asserting that they suffer present costs and burdens that are based on a fear of [future injury], so long as that fear is not 'fanciful, paranoid, or otherwise unreasonable.'" *Id.* at 1151. Such a theory failed, the Court explained, "because the harm respondents seek to avoid is not certainly impending." *Id.* To hold otherwise would "improperly water[] down the fundamental requirements of Article III." *Id.*

In other words, allegations of expenditures based on risk of future harm simply present the flip side of the *Clapper* coin. Without future harm that is "certainly impending," self-inflicted mitigation costs cannot confer standing. *See* CareFirst Br. 16-18 (collecting cases). Thus, plaintiffs' expenditures are of little relevance to standing; the pertinent question remains whether *Clapper*'s standard for risk of future harm has been satisfied. For the reasons discussed above, it has not.

Finally, although plaintiffs note CareFirst's post-breach offer to purchase identity theft protection services by way of background (Pls. Br. 2), they do not argue that this offer itself confers Article III

standing. For good reason: the fact that a business attempts to maintain goodwill by providing customers with insurance against a speculative but salient risk clearly does not establish that any harm is certainly impending. Moreover, as the Fourth Circuit recently held, "[c]ontrary to some of our sister circuits, we decline to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals." *Beck*, 2017 WL 477781, at *9. "To adopt such a presumption would surely discourage organizations from offering these services to data-breach victims, lest their extension of goodwill render them subject to suit." *Id.*; *cf.* Fed. R. Evid. 407 (precluding introduction of evidence of subsequent remedial measures to establish liability).

3. Plaintiffs cannot satisfy Article III simply by appending the word "privacy" to their allegations. While they assert, citing *Spokeo*, that an invasion of privacy is "a long standing tort capable of redressability" (Pls. Br. 15 (citing *Spokeo*, 136 S. Ct. at 1549)), they tellingly do not even attempt to show *how* the data breach here invaded their privacy, much less in a manner that bears a "close relationship"

(*Spokeo*, 136 S. Ct. at 1549) to an invasion that would support a common-law privacy tort.[3]

Plaintiffs thus get no mileage from this Court's dictum in *Hancock* that an "invasion of privacy" might amount to an intangible concrete harm. Pls. Br. 14-15 (citing *Hancock*, 830 F.3d at 514). This statement, understood in context, means that standing may be established on the basis of a claim of invasion of privacy akin to what would support a common-law privacy claim, not by merely incanting the term "privacy."

Abstract and inchoate "privacy" concerns of the kind plaintiffs raise have been repeatedly rejected as insufficient under Article III: as recent decisions have reiterated in both the statutory and common-law context, generalized assertions of "loss of privacy . . . are too abstract to establish Article III standing"; rather, a plaintiff must show resulting "damages or injury." *Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at *8 (E.D. Mo. July 12, 2016) (collecting cases); *accord, e.g.*, *Khan v. Children's Nat'l Health Sys.*, 2016 WL 2946165, at *6 (D. Md. May 19, 2016) (rejecting argument that hospital data breach in violation of state

[3] As CareFirst points out, plaintiffs' complaint does not contain any allegations of an invasion of privacy, which is reason enough to reject this belated theory of standing. CareFirst Br. 26.

statutes and common law "caused a loss of privacy that constitutes an injury in fact," because the plaintiff "has not identified any potential damages arising from such a loss and thus fails to allege a 'concrete and particularized injury'").

II. No-Injury Lawsuits Like This One Impose Unjustified Costs On Businesses.

For the reasons explained above, *Spokeo* and *Clapper* mandate dismissal of this case. The Supreme Court has made clear that a no-injury lawsuit based at most on anxiety about speculative future harm cannot go forward.

These legal principles governing standing do not exist in a vacuum. A failure to apply Article III's requirements rigorously has deeply troubling consequences for both defendants and the federal courts, especially in the context of data breach lawsuits like this one.

Enterprising members of the plaintiffs' bar have seized upon reported data breaches to try to extract millions of dollars from businesses whose systems have been attacked by thieves, foreign intelligence services,[4] or other hackers. Data breaches are an attractive

[4] *See, e.g.*, Michael Riley & Jordan Robertson, Bloomberg, *Chinese State-Sponsored Hackers Suspected in Anthem Attack* (Feb. 5, 2015),

target for plaintiffs' lawyers because they are widely reported by both the media and the victim companies themselves.[5] In addition, they are heavily investigated by both federal and state regulators—allowing plaintiffs' lawyers to simply jump on the bandwagon.

Accordingly, as one commentator put it, "[i]t's not a question of if you'll be hit with a data breach attempt, but when. And if it's successful, the fallout litigation is just as inevitable." Melissa Maleske, Law360, *The 6 Lawsuits All GCs Face After a Data Breach* (Dec. 9, 2015), https://www.law360.com/articles/735838/the-6-lawsuits-all-gcs-face-after-a-data-breach (noting that "[c]onsumer class actions are the most ubiquitous of post-breach litigation"). Moreover, a single data breach will often give rise to multiple putative class actions—as amply demonstrated by the breach at issue here. *See* CareFirst Br. 3-4

---

https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack.

[5] Nearly every State has a data breach notification law. *See, e.g.*, Nat'l Conf. of State Legislatures, *Security Breach Notification Laws* (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ("Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information.").

(discussing *Chambliss*, 189 F. Supp. 3d 564; *Unchageri*, 2016 WL 8255012); *see also, e.g.*, *In re SuperValu, Inc.*, 2016 WL 81792, at *2 (describing consolidation for pre-trial purposes of "four putative class actions brought by a total of twelve Plaintiffs . . . in federal courts in Illinois, Minnesota, and Idaho").

But in the absence of real-world injury (or a certainly impending one), these unproductive and abusive lawsuits simply generate fees for the lawyers rather than benefits for consumers or patients. The only "'victims'" of Article III's injury-in-fact requirement are, by definition, "persons or organizations who suffer no significant deprivation if denied the right to sue." *Gubala*, 2017 WL 243343, at *3. Yet lawsuits such as this one often result in *in terrorem* settlements that impose substantial costs on businesses even in the absence of real-world injury. Indeed, even when the defendant has strong defenses, these putative class actions are virtually never litigated on the merits. *See, e.g.*, *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting) ("A court's decision to certify a class . . . places pressure on the defendant to settle even unmeritorious claims."); Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*,

84 N.Y.U. L. Rev. 97, 99 (2009) ("With vanishingly rare exception, class certification sets the litigation on a path toward resolution by way of settlement, not full-fledged testing of the plaintiffs' case by trial.").

Plaintiffs' *amici* try to defend these abusive no-injury lawsuits on deterrence grounds, claiming they are necessary to avoid "giv[ing] a 'pass' to Corporate America" in the event of a data breach. NCL Br. 14; *see also* EPIC Br. 23-26. That argument fundamentally misunderstands Article III, which, of course, focuses on injury in fact to the plaintiff rather than deterrence to the defendant. Moreover, the plaintiffs' assumptions are wrong for multiple reasons.

First, enforcing the injury-in-fact requirement does nothing to foreclose plaintiffs who have been actually harmed or placed at substantial risk of future harm by a data breach from bringing lawsuits in federal court. For this same reason, plaintiffs' *amicus* misunderstands what is at stake in this case when it argues that liability "force[s] defendants to internalize the full measure of the damages that they cause and take sufficient care to prevent future harms." EPIC Br. 24-25. There is no dispute that *Spokeo* allows injured plaintiffs to impose "the full measure of the damages" on responsible

companies. Rather, the question in this case is whether uninjured plaintiffs may attempt to extract large statutory penalties, which impose far beyond any "full measure of damages" on defendant companies.

In addition, *amici*'s implication that businesses will not take adequate care to prevent data breaches absent no-injury class actions is simply not credible. Businesses' primary motivation for avoiding data breaches surely comes from the substantial public relations harm and loss of goodwill that follows any breach of their customers' data. Moreover, data security is already heavily regulated under a substantial number of federal and state laws, and public officials rigorously enforce those laws. *See generally* Institute for Legal Reform, *A Perilous Patchwork: Data Privacy And Civil Liberty In The Era Of The Data Breach* (Oct. 2015), http://www.instituteforlegalreform.com/uploads/sites/1/APerilousPatchwork_Web.pdf. Both federal agencies and state attorneys general have actively pursued companies that have suffered data breaches, requiring "significant penalties and corrective actions" in order to settle their enforcement actions. *Id.* at 11.

For instance, the FCC required a $3.5 million settlement and corrective action from TerraCom and YourTel America in July 2015. *See* Federal Communications Commission, TerraCom & YourTel to Pay $3.5M For Privacy Breach Violations, https://www.fcc.gov/document/terracom-yourtel-pay-35m-privacy-breach-violations. In the healthcare context in particular, the Office of Civil Rights (OCR), an agency under the umbrella of HHS, "has increased its enforcement efforts" in recent years, reaching, for example, a $4.8 million settlement and corrective action plan with Columbia University and New York Presbyterian Hospital. *A Perilous Patchwork*, *supra*, at 15 (citing Press Release, U.S. Department of Health and Human Services–Office for Civil Rights, Data Breach Results in $4.8 Million HIPAA Settlements (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html).

It is no wonder then that data breaches impose substantial costs on American businesses. As the Chamber's Institute for Legal Reform has reported, "American businesses spend an average of $6.5 million on a single data breach, including the price of notifying potentially affected individuals and ensuing legal costs." Institute for Legal Reform, *Data Privacy*, http://www.instituteforlegalreform.com/issues/data-privacy.

Given the already potentially staggering costs of data breaches, along with the enormous reputation damage they can cause, businesses are fully incentivized to invest in reasonable care of the data in their possession without the additional burden of no-injury class actions. Indeed, that is why businesses across industries, from insurance to the "Internet of Things,"[6] are investing heavily in cybersecurity and working collaboratively with federal and state governments to protect themselves and their customers from the sophisticated threats they face. *See, e.g.*, Nat'l Inst. of Standards & Tech., *Cybersecurity "Rosetta Stone" Celebrates Two Years of Success* (Feb. 18, 2016), https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success (describing successful cybersecurity risk management framework that resulted from "intensive collaboration with industry" and that has now been widely adopted in the private sector).

[6] *See, e.g.*, Jacob Morgan, Forbes, *A Simple Explanation Of 'The Internet Of Things,'* (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#44e250666828.

In short, the mere occurrence of a data breach should not automatically enable the plaintiffs' bar to launch class-action litigation designed to wrest massive settlements from businesses in the absence of actual harm.

CONCLUSION

The judgment below should be affirmed.

Dated: February 15, 2017

Respectfully submitted,

Kate Comerford Todd
Steven P. Lehotsky
Warren Postman
U.S. CHAMBER LITIGATION CENTER
1615 H Street, N.W.
Washington, DC 20062
(202) 463-5337

s/ Andrew J. Pincus
Andrew J. Pincus
Archis A. Parasharami
Stephen C.N. Lilley
Daniel E. Jones
MAYER BROWN LLP
1999 K Street, N.W.
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Attorneys for Amicus Curiae
The Chamber of Commerce of the United States of America

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I hereby certify that this brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and 32(a)(7)(B) because it contains 5,204 words, excluding the parts exempted by Fed. R. App. P. 32(a)(7)(B)(iii) and Cir. R. 32(a)(1). I further certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because the brief was prepared in 14-point Century Schoolbook font using Microsoft Word.

Dated: February 15, 2017

/s/ Andrew J. Pincus
Andrew J. Pincus

CERTIFICATE OF SERVICE

I hereby certify, pursuant to Fed. R. App. P. 25(c) and Cir. R. 25(a), that on February 15, 2017, the foregoing was electronically filed with the Clerk of the Court using the CM/ECF system, which will send a notification to the attorneys of record in this matter who are registered with the Court's CM/ECF system.

Dated: February 15, 2017

/s/ Andrew J. Pincus
Andrew J. Pincus