No. 17-641

In the Supreme Court of the United States

CAREFIRST, INC., doing business as Group Hospitalization and Medical Services, Inc., doing business as CareFirst of Maryland, Inc., doing business as Carefirst BlueCross BlueShield, doing business as CareFirst BlueChoice, Inc., *et al.*,
Petitioners,

v.

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

On Petition for a Writ of Certiorari to the United States Court of Appeals for District of Columbia Circuit

REPLY BRIEF FOR PETITIONERS

Robert D. Owen
Francis X. Nolan, IV
EVERSHEDS
SUTHERLAND (US) LLP
1114 Avenue of the Americas
The Grace Building
40th Floor
New York, NY 10036
T. 212.389.5000
F. 212.389.5099

Matthew O. Gatewood
Counsel of Record
EVERSHEDS
SUTHERLAND (US) LLP
700 Sixth St., NW, Suite 700
Washington, D.C. 20001
T. 202.383.0122
F. 202.637.3593
MatthewGatewood@
eversheds-sutherland.com

Counsel for Petitioners

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTION

REPLY BRIEF FOR PETITIONERS

The D.C. Circuit applied a standard to evaluate Respondents' alleged threatened injuries that obviates the requirement that those future injuries be imminent. In doing so, the court of appeals departed from this Court's guidance on standing. Respondents do not allege that their injuries have even an objectively reasonable likelihood of occurring (the standard the Court rejected as not rigorous enough in *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013)), let alone that a substantial risk of injury exists. The inadequate application of the substantial risk test by the court of appeals effectively eliminates the need for a plaintiff to plead that a threatened injury is imminent to bring a federal case.

Contrary to Respondents' assertions, federal courts are vexed with articulating what constitutes standing for alleged threatened injury, particularly in the context of lawsuits brought by victims of data breaches against the companies that held the accessed data. The answer to the question in these cases now depends more on the venue of an action than on established standards, including this Court's jurisprudence. The D.C. Circuit held that Respondents alleged enough facts to confer standing, but at a minimum, the Third, Fourth, and Eighth Circuits would have found they did not.

Respondents downplay the significance of the D.C. Circuit's conclusion despite a rising tide of data breach class actions. Should the Court leave the D.C. Circuit's opinion undisturbed, any individual who pleads that her data was exposed in a breach will be able to maintain a lawsuit against the company that held that

data, even if the plaintiff suffered no harm whatsoever. That scenario cannot be reconciled with the fundamental principle that an injury in fact must be actual or *imminent*. The Court should grant certiorari.

A. A Circuit Court Split Exists.

Respondents ignore the conflicting holdings from the courts of appeals (Pet. Cert. 10-15), a split that some courts have explicitly acknowledged, *see, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 273 (4th Cir. 2017).

Respondents' attempts to reconcile the circuits are unconvincing. For example, they argue that the Third Circuit does not differ from the D.C. Circuit because *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d. Cir. 2011), preceded *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625 (3d Cir. 2017). But *In re Horizon Healthcare* did not reverse *Reilly*, and its holding is not relevant here. In *In re Horizon Healthcare*, the Third Circuit did not analyze what a plaintiff must plead to show a substantial risk of future harm, and instead issued a limited holding, stating "that the improper disclosure of one's personal data in violation of [the Fair Credit Reporting Act] is a cognizable injury for Article III standing purposes." *Id.* at 641. Respondents' argument that *In re Horizon Healthcare* means that "the Third Circuit stands shoulder-to-shoulder with the D.C. Circuit in its opinion that allegations of a data breach by data thieves creates a substantial risk of future injury," (Opp'n 17), is wrong.

Respondents also incorrectly rely on the Fourth Circuit's decision in *Wikimedia Found. v. Nat'l Sec. Agency*, 857 F.3d 193 (4th Cir. 2017). There, the court

found that "the interception of Wikimedia's communications is an actual injury that has already occurred," *id*. at 210, and that, "Wikimedia pleaded an actual and ongoing injury, which renders *Clapper's* certainly-impending analysis inapposite here." *Id.* at 211.

The more applicable Fourth Circuit decision is more recent and much closer on the facts. In *Beck*, the plaintiffs failed to allege a certainly impending harm *or* a substantial risk of harm. 848 F.3d at 275-76.

The *Beck* court first found that there was no certainly impending risk of future harm because that would require the court to "assume that the thief targeted the stolen items for the personal information they contained. * * * [T]he thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This 'attenuated chain' cannot confer standing." *Id.* at 275. Like the Respondents' allegations of future injury, the allegations in *Beck* were not certainly impending.

In considering whether the plaintiffs in *Beck* had alleged a substantial risk of future harm, the Fourth Circuit looked to the plaintiffs' representations that: (1) one-third of health-related data breaches result in identity theft; (2) the defendants spent money trying to avoid the risk of data breaches; and (3) the defendants offered credit monitoring services to the plaintiffs following the breach, ostensibly with the expectation that identity theft (and thus future injury) would

occur.[1] But those allegations, even if accepted as true, at most made the possibility of future identity theft "reasonably likely," insufficient to satisfy the imminence requirement for an injury in fact. *Id.* at 276. Contrast that finding with the D.C. Circuit's conclusion that a substantial risk of harm exists "simply by virtue of the hack and the nature of the data." App. 16. *Beck* is irreconcilable with the D.C. Circuit's opinion here.

The Eighth Circuit also would have decided this case differently than did the D.C. Circuit. In *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017), the court affirmed dismissal of the claims of all but one plaintiff, finding that the complaint did not allege a substantial risk of future identity theft or credit card fraud.[2] The court distinguished between the "mere possibility" of future harm and a substantial risk of future harm after considering a Government Accounting Office report cited in the plaintiffs' complaint. *Id.* at 771. "Although the report acknowledges that there are some cases in which a data breach appears to have resulted in identity theft, it concludes based on the 'available data and information' that 'most breaches have not resulted in detected incidents of identity theft,'" and further

---

[1] The Fourth Circuit highlighted the circuit court split on this particular point. *Beck*, 848 F.3d at 276 ("Contrary 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.").

[2] The Eighth Circuit did reverse dismissal as to one plaintiff, but on a theory of a *present* injury sustained as a result of the defendants' conduct, *In re SuperValu*, 870 F.3d at 768, a theory that the D.C. Circuit expressly declined to consider. App. 10 n.2.

supports the conclusion that credit card fraud is unlikely. *Id.*

The Eighth Circuit would thus certainly disagree with the D.C. Circuit's conclusion that mere "unauthorized access" to Respondents' "members' names, birth dates, email addresses and subscriber identification number[s] * * * creates a material risk of identity theft" sufficient to satisfy the substantial risk standard. App. 14. Even if the Eighth Circuit had accepted Respondents' flimsy (and disproven) allegations of accessed Social Security numbers as true, under its *SuperValu* analysis, it would have concluded there was only a "possibility" of future identity theft. *In re SuperValu*, 870 F.3d at 770 (finding insufficient allegations to support "the otherwise bare assertion that '[d]ata breaches facilitate identity theft'"). On the other hand, the D.C. Circuit found that "it is plausible * * * to infer that [the data thief] has both the intent and the ability to use that data for ill," (App. 15), despite no supporting allegations in the complaint. The Eighth Circuit court would also find a risk of using the accessed information to impersonate one of the Respondents, *id.* at 14, to be even more remote. *See Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) ("[A] speculative or hypothetical risk is insufficient.").

Respondents assert that CareFirst "seek[s] to carve out and create standing requirements particular to data breach cases." Opp'n 14. On the contrary, CareFirst seeks the Court's guidance on what a plaintiff must allege to establish an injury in fact for an allegedly threatened injury, a scenario that frequently arises because of the increase in the number of data

breach cases. Respondents also claim that, "[f]or decades the circuits have established that they are more than capable of applying this Court's standing jurisprudence to cases and controversies." *Id.* 1. This non-sequitur ignores the Court's recent opinions on Article III standing involving emerging contexts, such as allegations of injury arising from modern day surveillance (*Clapper*) and information disseminated on the internet (*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)). CareFirst does not ask the Court to establish a new standard, but to reaffirm that a substantial risk of threatened injury cannot be sufficient to confer Article III standing unless that risk is indeed actual or imminent. This case provides an ideal opportunity to provide that clarity.

B. The D.C. Circuit Erred.

CareFirst does not take the position that *Clapper* "purport[ed] to alter the 'substantial risk' standard as a sufficient means for alleging future harm." Opp'n 7. CareFirst's position, as set forth in the Petition, is that the circuit court lowered the "substantial risk" standard by creating implausible scenarios of possible future harm, most of which do not rely on specific factual allegations in the complaint. Nor does CareFirst "ignore" *Susan B. Anthony List v. Driehaus* ("*SBA List*"), 134 S. Ct. 2334 (2014), as Respondents suggest. Opp'n at 8. In *SBA List*, this Court applied the substantial risk test to factual allegations easily distinguishable from those considered by the court of appeals. The plaintiffs there alleged a credible threat of the Ohio Election Commission bringing enforcement proceedings against them, in addition to a threat of criminal prosecution, based on the plaintiffs' future

planned exercise of free speech. 134 S. Ct. at 2346. The Court considered the threats credible because, *inter alia*, the Commission had taken action against one of the plaintiffs for similar statements in the past. *Id.* at 2345 ("there is every reason to think that similar speech in the future will result in similar proceedings"). The future risk to the plaintiffs in *SBA List* was, therefore, more tangible, predictable, and likely to occur than here. It was plausible. The threat of future harm to Respondents, on the other hand, rests in the hands of unidentified third-party actors who have taken no adverse action against Respondents in the nearly four years since the theft. There is not even a reasonable likelihood that such harm will occur, must less a substantial risk of harm.

The D.C. Circuit departed from the standards enunciated in *Clapper* and *SBA List* in other ways. The court of appeals held that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." App. 16. The court offered no legal or factual support for this bold holding. The court of appeals read into the complaint allegations that the data breach accessed Respondents' Social Security numbers. The district court had concluded otherwise and noted that even if there were such an allegation, CareFirst submitted a sworn declaration in support of its motion to dismiss proving that Respondents' allegations were untrue. App. 22, 24 n.1.

The circuit court also created a theory of future injury not set forth in the complaint. Specifically, the D.C. Circuit imagined a scenario in which the unknown thief would impersonate members of the putative class

to receive health care services. *See id.* at 6. Rather than attempt to justify or explain that novel theory, Respondents make much of the alleged injury to two of the putative class action plaintiffs, the Tringlers. Opp'n 3, 14 n.3, 24-25. That reliance is misplaced. Most importantly, the circuit court did not base its finding of standing on the Tringlers' alleged injury.[3] App. 10 n.2 ("Because we conclude that all plaintiffs, including the Tringlers, have standing to sue CareFirst based on their heightened risk of future identity theft, we need not address the Tringlers' separate argument as to past identity theft.").

Furthermore, had the court relied on the alleged injury to the Tringlers to find standing, it would have dismissed the claims of the five other putative class representatives, none of whom alleged that they suffered a present injury. The Tringlers only represent one of three proposed subclasses, so the complaint would have been dismissed as to those subclasses as well. *See Warth v. Seldin*, 422 U.S. 490, 502 (1975). The D.C. Circuit also left intact the district court's finding that the complaint did not plausibly allege that the injury to the Tringlers arose from the allegedly stolen information. App. 31.

---

[3] Nor did the Circuit Court rely, as Respondents imply (Opp'n 27), on allegations of statutory harm. App. 10 n.2 ("For the same reason, we will not address the other theories of standing advanced by plaintiffs or their amici, including the theory that CareFirst's alleged violation of state consumer protection statutes was a distinct injury in fact.").

The circuit court's holding, if left undisturbed, will eviscerate any workable standard for evaluating when a threat of a future harm is sufficiently imminent to satisfy Article III standing, and will open the door to a flood of no-injury class actions arising from virtually every data breach. The damage will not be limited to data breach cases, however, as Respondents are correct that standing jurisprudence is not industry- or claim-specific.

CONCLUSION

For the foregoing reasons, this Court should grant the Petition for Writ of Certiorari.

Respectfully submitted,

Robert D. Owen
Francis X. Nolan, IV
EVERSHEDS SUTHERLAND (US) LLP
1114 Avenue of the Americas
The Grace Building
40th Floor
New York, NY 10036
T. 212.389.5000
F. 212.389.5099

Matthew O. Gatewood
Counsel of Record
EVERSHEDS SUTHERLAND (US) LLP
700 Sixth St., NW
Suite 700
Washington, D.C. 20001
T. 202.383.0122
F. 202.637.3593
MatthewGatewood@eversheds-sutherland.com

Counsel for Petitioners

JANUARY 2018