NO. 18-225

In the
Supreme Court of the United States

ZAPPOS.COM, INC.,

Petitioner,

v.

THERESA STEVENS, DAHLIA HABASHY, PATTI HASNER, SHARI SIMON, STEPHANIE PRIERA, KATHRYN VORHOFF, DENISE RELETHFORD, and ROBERT REE,

Respondents.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

REPLY BRIEF FOR PETITIONER

STEPHEN J. NEWMAN
JULIA B. STRICKLAND
BRIAN C. FRONTINO
BRENDAN S. EVERMAN
STROOCK & STROOCK & LAVAN LLP
2029 Century Park East
Suite 1800
Los Angeles, CA 90067

PAUL D. CLEMENT
Counsel of Record
ERIN E. MURPHY
MATTHEW D. ROWEN
KIRKLAND & ELLIS LLP
655 Fifteenth Street, NW
Washington, DC 20005
(202) 879-5000
paul.clement@kirkland.com

Counsel for Petitioner

November 19, 2018

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

REPLY BRIEF

Respondents accuse Zappos of "manufactur[ing a] circuit split," BIO.13, but rhetoric cannot change reality: The circuits themselves have acknowledged that they "are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft." *Beck v. McDonald*, 848 F.3d 262, 273 (4th Cir. 2017). That question—whether individuals who themselves allege no identity theft from a data breach can nonetheless plead Article III injury based on an alleged risk of *future* identity theft stemming from a breach—is the sole issue the Ninth Circuit decided here. The question not only has divided the circuits, but demands a uniform, nationwide answer, as data breaches involve customers in multiple circuits, and the prevalence of data breaches (and data breach litigation) only increases each year. The Court should grant certiorari.

I. Respondents' Attempts To Minimize The Circuit Split Are Unavailing.

Respondents contend that the circuit split detailed at length in the petition is a manufactured illusion. The lower courts beg to differ. In 2017, a district court in the Eleventh Circuit counted "three circuits" that had "held that a risk of future identity theft can constitute an injury in fact," and "[t]hree others" that had "held that it does not." *Wilding v. DNC Servs. Corp.*, No. 16-61511-CIV, 2017 WL 6345492, at *7 (S.D. Fla. Aug. 25, 2017); *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 392 (6th Cir. 2016) (Batchelder, J., dissenting) (highlighting "circuit split"). Since then, "the circuit

split has deepened." *Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 338 (W.D.N.Y. 2018). The D.C. Circuit joined the Sixth, Seventh, and Ninth Circuits in the former camp, and the Eighth Circuit joined the First, Third,[1] and Fourth Circuits in the latter camp. Pet.13-18. The Second Circuit also has held, albeit in a non-precedential order, that plaintiffs failed to plead Article III injury where they alleged only a "risk of future identity fraud" but no actual identity theft after their "credit card information was stolen." *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017).

Courts are not alone in recognizing this entrenched circuit split; commentators repeatedly have identified it too. *See, e.g.*, Alex Bossone, *The Battle Against Breaches: A Call for Modernizing Federal Consumer Data Security Regulation*, 69 Fed. Comm. L.J. 227, 228 (2018) ("[C]ircuit courts are split over whe[ther] an individual may recover for a data breach claim … against a company from which the customers' data was stolen, even where the data has not yet been harmfully used."); Kimberly Fasking, Beck v. McDonald*: The Waiting Game—Is an Increased Risk of Future Identity Theft an Injury-in-Fact for Article III Standing?*, 41 Am. J. Trial Advoc. 387, 389 (2017) ("Currently, a circuit split exists on the issue of whether the victim of a data breach has Article

[1] The Third Circuit actually appears to have adopted a third approach, with standing turning on the nature of the claim. *Compare In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 639 n.20 (3d Cir. 2017) (finding standing on mere allegation of risk of future injuries for a FCRA claim), *with Reilly v. Ceridian Corp.*, 664 F.3d 38, 40-42 (3rd Cir. 2011) (finding similar allegations insufficient for common law claim).

III standing to sue the entity with whom she entrusted her personally identifying information when that information has not yet been used to commit fraud."); Lee J. Plave & John W. Edson, *First Steps in Data Privacy Cases: Article III Standing*, 37 Franchise L.J. 485, 487 (2018) ("[F]ederal courts are split on whether the threat of future harm attributable to a data breach gives a plaintiff standing to sue the company that allegedly failed to protect his or her personally identifiable information.").

Respondents protest that each of these decisions purports to "apply the same legal standard for assessing injury-in-fact." BIO.10; *see* BIO.10-21. But the fact that all circuits start with broad principles drawn from this Court's cases is neither surprising nor material. Despite starting from the same general legal principles, one set of circuits holds that an increased risk of future identity theft *suffices* under those general principles and Article III, whereas another set holds that it does not. That disagreement is not attributable to different facts, but rather stems from fundamentally different views of what Article III and this Court's caselaw require in this recurring situation, which is pretty much the definition of a circuit split.

For instance, the D.C. Circuit has held that plaintiffs who alleged "the theft of social security or credit card numbers in the data breach" pleaded enough for Article III injury, even though they did not allege that they had suffered any actual identity theft. *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017). The Sixth Circuit likewise has held that plaintiffs whose "names, dates of birth, … Social

Security numbers, and driver's license numbers" allegedly were compromised in a data breach pleaded enough for Article III injury based solely on "the theft of their personal data," even though no plaintiffs alleged that they had suffered any actual identity theft. *Galaria*, 663 F. App'x at 386-89. By contrast, the Eighth Circuit has held that plaintiffs could *not* satisfy Article III where they alleged that "hackers stole [their] … names, credit or debit card account numbers, … and personal identification numbers," because they did not allege any actual "misuse of any such data." *In re SuperValu, Inc.*, 870 F.3d 763, 766-72 (8th Cir. 2017).

Each of those cases was decided on the pleadings. *See Attias*, 865 F.3d at 623; *Galaria*, 663 F. App'x at 387; *In re SuperValu*, 870 F.3d at 765-66. Each involved allegations that data thieves intentionally targeted sensitive personal information, including payment information. Yet two circuits held that the plaintiffs pleaded enough for Article III, whereas one circuit held that the plaintiffs did not. While respondents quibble over just how far the Eighth Circuit's decision in *SuperValu* goes, *see* BIO.16, the salient point is that all three courts considered materially indistinguishable allegations, and the Eighth Circuit found no standing, while the D.C. and Sixth Circuits found standing.

And the split is deeper still. The Fourth Circuit has held that plaintiffs who do not allege that their information "ha[s] been misused" following a data breach fail to "'establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against it.'"

Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 621-22 (4th Cir. 2018) (citing *Beck*, 848 F.3d at 274-75). By contrast, the Ninth Circuit here "held that respondents 'sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers *will commit* identity fraud or identity theft,'" even though not one of the individuals "'at issue' in the appeal" alleged any *actual* identity theft. BIO.9 & n.5 (emphasis added) (quoting Pet.App.14, 16-17). Moreover, whereas the Fourth Circuit considered the passage of time without any meaningful identity theft relevant in holding that the alleged future harm was not imminent, the Ninth Circuit refused to do so here. *Compare Beck*, 848 F.3d at 274, *with* Pet.App.15-16 & n.12.

Respondents attempt to complicate the picture in the Fourth Circuit, *see* BIO.12 n.6, 16 n.7, but their efforts are unavailing. *Hutton*, which respondents relegate to a footnote, could not be clearer. The plaintiffs there had standing because they "allege[d] that they ha[d] already suffered actual harm in the form of identity theft and credit card fraud." *Hutton*, 892 F.3d at 622. By contrast, the *Beck* plaintiffs *lacked* standing because they "alleged only a threat of future injury." *Id.* at 621-22 (distinguishing *Beck*).

Unable to change the reality of the circuit split, respondents try to change the subject. Respondents insist that "[n]o court has asserted that a *substantial* risk of identity theft is insufficient for standing." BIO.12 n.6. But the problem is that courts disagree about what it takes to make a risk of identity theft "substantial." In some circuits, the mere fact of a data breach is enough; in others, it is not. Which circuits

have the better of that argument is undeniably a "legal question for this Court to resolve." BIO.1.

II. This Is An Excellent Vehicle To Resolve The Entrenched Circuit Split.

Contrary to respondents' contentions, the only "facts" relevant to this petition are not subject to "dispute." BIO.1. As the Ninth Circuit made clear, "the plaintiffs who are the focus of this appeal … did not" "allege[] that the hackers used stolen information about them to conduct subsequent financial transactions." Pet.App.4. "This appeal concerns claims based on the hacking incident itself, *not any subsequent illegal activity*." Pet.App.4 (emphasis added).

To be sure, two *other* individuals alleged that "someone used" their personal information to make "fraudulent charges" to their accounts. BIO.5-7, 30. But as respondents admit, BIO.9 n.5, those two later-added plaintiffs "are not at issue in this appeal," Pet.App.14, as the district court ruled that those two plaintiffs—but *only* those two—alleged injuries sufficient for Article III, Pet.App.33-38. Accordingly, those two individuals are not among the respondents, and their claims have no bearing on present proceedings. Indeed, if anything, the fact that the district court expressly differentiated those two individuals makes this petition a particularly good vehicle for resolving the question presented, as it confirms beyond doubt that none of the respondents at issue in these proceedings has alleged any "actual financial harm or that [her] personal information has been disseminated over the Internet." Pet.App.66.

That is certainly true of respondents themselves. While respondents Patti Hasner and Zetha Nobles did allege that "fraudsters hijacked" their "email accounts," BIO.29; *see* BIO.5-6, they did not allege that they suffered any concrete injury as a result. All they claimed is that the hacker "sent unauthorized advertisements to others from the[ir] accounts." Pet.App.66 n.3; *see* BIO.5. Hence, the Ninth Circuit held *not* that Hasner and Nobles alleged actual injury, but that their allegations "support [respondents'] contention that the hackers accessed information that *could be used* to help commit identity fraud or identity theft," a possibility that the court considered "sufficient[] … under *Krottner* [*v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010)]." Pet.App.14 (emphasis added).

Finally, respondents seek to muddy the waters by insisting that Zappos's method of storing customers' data is in dispute. BIO.28-29. That is a non-sequitur. What petitioner did before the breach has no relevance to whether respondents alleged or suffered Article III injury from the breach.

III. The Decision Below Is Wrong.

Plaintiffs seeking redress for alleged injuries yet to occur face a "more rigorous burden" than do plaintiffs seeking redress for injuries allegedly already suffered. *United Transp. Union v. ICC*, 891 F.2d 908, 913 (D.C. Cir. 1989). While federal courts must accept as true allegations "of facts, historical or otherwise demonstrable," that obligation does not extend to claims "that are really predictions." *Id.* at 912. Nor could it. To satisfy Article III, an alleged injury "must be concrete in both a qualitative and temporal sense."

Whitmore v. Arkansas, 495 U.S. 149, 155 (1990). And to be concrete, an alleged future harm must be substantially "certain[]" to occur. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409-10 (2013). Accordingly, "[a]llegations of possible future injury do not satisfy the requirements of Article III." *Whitmore*, 495 U.S. at 158.

Yet "possible future injury" is all respondents alleged here. Of the 24 million customers potentially affected by the 2012 breach, 0.00001% of them have ever complained, either informally to Zappos or in formal pleadings, that their personal information was misused as a result of the breach. Pet.21. Respondents do not dispute that. Instead, they insist that it is irrelevant because they "pleaded that victims 'may not see the full extent of identity theft or identity fraud for years'" and that "'stolen data may be held' for some time before criminals trade it on the 'cyber black-market' indefinitely." BIO.32 (footnote omitted). But an injury that "may" take place "some time" in the future, BIO.32, is obviously *not* temporally "concrete."

Clapper could not make that clearer. The Court in *Clapper* went out of its way to explain that even an "objectively reasonable likelihood" of injury is not enough. 568 U.S. at 410. That is because Article III demands, at a minimum, "alleg[ations] that the plaintiff 'has sustained or *is immediately in danger* of sustaining some direct injury.'" *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) (emphasis added) (quoting *Massachusetts v. Mellon*, 262 U.S. 447, 488 (1923)). And while "imminence" cannot be reduced to a mathematical formula, *Clapper*, 568 U.S. at 409, an infinitesimal incidence of injury after six years—two

non-respondents out of 24 million potentially affected individuals—plainly does not satisfy Article III. *See Beck*, 848 F.3d at 276 (alleged 33% likelihood of identity theft insufficient because "over 66% … will suffer no harm").

The Ninth Circuit rejected that reasoning on the ground that the *Beck* plaintiffs "did not allege that the 'thief intentionally targeted the personal information compromised in the data breaches,'" whereas the plaintiffs here "allege that hackers specifically targeted their PII on Zappos's servers." Pet.App.17 n.13 (quoting *Beck*, 848 F.3d at 274). But it is the rare hacker who inadvertently obtains personal information, so if all it takes to satisfy Article III is an "intentional targeting" allegation, then every data breach plaintiff will simply add such an allegation. That cannot be the law. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (standing is not a "mere pleading requirement[]").

Finally, respondents assert that "no authority" contradicts their position that a plaintiff can satisfy Article III by pointing to the injuries of *other*, "similarly situated victims." BIO.30. But when at most two individuals out of a universe of 24 million suffer concrete injury, the few are not "similarly situated" to the many. Moreover, it is black-letter law that "[t]o be entitled to" monetary relief in federal court, every person must show that he suffered (or will imminently suffer) an injury that is not only concrete, but particularized as to him. *Tyson Foods, Inc. v. Bouaphakeo*, 136 S. Ct. 1036, 1045-46 (2016); *see also Town of Chester v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1651 (2017) (to obtain "money judgments in their own

names," all parties must "have Article III standing"). And to be particularized, an injury "must affect the plaintiff in a personal and individual way." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan*, 504 U.S. at 560 n.1); *see* Pet.20. Thus, even if others allege actual identity theft particularized to them, a plaintiff's failure to allege particularized injury *of his own* is fatal under Article III.

IV. This Issue Is Important And Ripe For Resolution.

Respondents cannot contest that data breaches (and data breach litigation) are on the rise. Pet.28-29. Nor can they deny that data breaches typically involve customers residing across the country and across the circuits, which makes a circuit split both intolerable and an invitation for forum shopping. Respondents claim instead that "defendants that 'design their systems properly'" have nothing to fear, because such defendants "will prevail on the merits." BIO.27. But that is no answer to concerns about a lack of standing, and it is cold comfort to companies forced to litigate when the only party suffering concrete injury from a cyberattack is the company/defendant itself. *See* Br. of *Amicus Curiae* The Chamber of Commerce of the United States of America 11-19. Moreover, this case makes plain that "[e]stablished legal tools such as motions to dismiss," BIO.27, are currently unable to separate the wheat from the chaff or to protect victimized companies from protracted litigation.

Respondents next contend that this Court's intervention is unnecessary because some courts have resorted to "statutorily defined injuries-in-fact" to circumvent the question presented. BIO.25-26; *see In*

re Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639-40 & n.20 (3d Cir. 2017). In reality, that highlights the disarray in the circuits, *see supra* n.1, and the need for review. Creative plaintiffs' attorneys can almost always find a statutory damages theory that fits the facts of their data breach (at least at the pleadings stage), but alleging a statutory violation is no substitute for alleging injury in fact.

The stakes implicated here are substantial. As this case lays bare, most data breaches affect thousands if not millions of individuals, and thus beget sprawling class actions. If companies are forced to spend time and money defending such suits even without "a concrete factual context conducive to a realistic appreciation of the consequences of judicial action," *Valley Forge Christian Coll. v. Ams. United for Separation of Church and State, Inc.*, 454 U.S. 464, 472 (1982), then the costs of such victimless suits will be a substantial drag on innovative companies no matter what they do to ensure that nearly inevitable hacking is addressed promptly and does not result in actual injuries. Insisting on actual injury, by contrast, gets the incentives right. Companies will have every incentive to invest in protecting data and responding quickly to prevent both injuries and lawsuits, neither of which should be inevitable.

In the end, respondents hang their hat on the truism that the facts of every data breach case are different. Of course they are. But they are not different in ways that explain the differing results courts have reached. Nor are they different in a way that obviates the need for this Court to resolve that square circuit conflict. A decision rejecting the notion

that merely being a customer of a company subject to a data breach is enough to satisfy Article III would cut across all factual scenarios and ensure that federal courts are adjudicating only concrete disputes over which they have jurisdiction.

CONCLUSION

For the foregoing reasons, the Court should grant the petition.

Respectfully submitted,

STEPHEN J. NEWMAN
JULIA B. STRICKLAND
BRIAN C. FRONTINO
BRENDAN S. EVERMAN
STROOCK & STROOCK & LAVAN LLP
2029 Century Park East
Suite 1800
Los Angeles, CA 90067

PAUL D. CLEMENT
Counsel of Record
ERIN E. MURPHY
MATTHEW D. ROWEN
KIRKLAND & ELLIS LLP
655 Fifteenth Street, NW
Washington, DC 20005
(202) 879-5000
paul.clement@kirkland.com

Counsel for Petitioner

November 19, 2018