No. _____

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

PETITION FOR WRIT OF CERTIORARI

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

August 20, 2018

QUESTION PRESENTED

Whether individuals whose personal information is held in a database breached by hackers have Article III standing simply by virtue of the breach even without concrete injury, as the Third, Sixth, Seventh, Ninth, and D.C. Circuits have held, or whether concrete injury as a result of the breach is required for Article III standing, as the First, Second, Fourth, and Eighth Circuits have held.

PARTIES TO THE PROCEEDING

Petitioner Zappos.com, Inc. ("Zappos") was the defendant in the district court and appellee below.

Respondents Theresa Stevens, Dahlia Habashy, Patti Hasner, Shari Simon, Stephanie Priera, Kathryn Vorhoff, Denise Relethford, and Robert Ree were plaintiffs in the district court and appellants below.

CORPORATE DISCLOSURE STATEMENT

Zappos is a wholly owned subsidiary of Amazon.com, Inc., a publicly held corporation.

TABLE OF CONTENTS

QUESTION PRESENTED i
PARTIES TO THE PROCEEDING ii
CORPORATE DISCLOSURE STATEMENT iii
TABLE OF AUTHORITIES vii
PETITION FOR WRIT OF CERTIORARI 1
OPINIONS BELOW 3
JURISDICTION 4
CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED 4
STATEMENT OF THE CASE 4
A. Factual Background 4
B. Procedural History 5
1. District Court Proceedings 5
2. The Decision Below 8
REASONS FOR GRANTING THE PETITION 11
I. There Is An Acknowledged Split Of Authority On The Question Presented 13
II. The Decision Below Cannot Be Reconciled With This Court's Precedent 18
A. Future Injuries Must Be "Certainly Impending" To Satisfy Article III 18
B. Respondents Did Not Allege Substantial Risk That Harm Will Occur 21
III. This Case Is An Ideal Vehicle To Resolve The Split On This Frequently Recurring And Exceedingly Important Issue 28
CONCLUSION 32

APPENDIX

Appendix A

Order and Amended Opinion, United States Court of Appeals for the Ninth Circuit, *Stevens v. Zappos.com, Inc.*, No. 16-16860 (Apr. 20, 2018) App-1

Appendix B

Order, *Stevens v. Zappos.com, Inc.*, United States Court of Appeals for the Ninth Circuit No. 16-16860 (May 8, 2018) App-20

Appendix C

Order, *Stevens v. Zappos.com, Inc.*, United States Court of Appeals for the Ninth Circuit, No. 16-16860 (July 6, 2018) App-22

Appendix D

Stipulation and Order Granting Dismissal with Prejudice as to All Claims for Plaintiffs, United States District Court for the District of Nevada, *In re Zappos.com, Inc., Customer Data Security Breach Litigation*, No. 3:12-cv-00325 (Sept. 13, 2016) App-24

Appendix E

Order, United States District Court for the District of Nevada, *In re Zappos.com, Inc., Customer Data Security Breach Litigation*, No. 3:12-cv-00325 (May 13, 2016) App-26

Appendix F

Order, United States District Court for the District of Nevada, *In re Zappos.com, Inc., Customer Data Security Breach Litigation*, No. 3:12-cv-00325 (June 1, 2015) App-47

Appendix G

U.S. Const. art. III, §§ 1-2 ..... App-73

TABLE OF AUTHORITIES

Cases

Allen v. Wright,
468 U.S. 737 (1984)..... 19

Attias v. Carefirst, Inc.,
865 F.3d 620 (D.C. Cir. 2017)..... 10, 16

Beck v. McDonald,
848 F.3d 262 (4th Cir. 2017)..... 13, 14, 15, 26

Clapper v. Amnesty Int'l USA,
568 U.S. 398 (2013)..... *passim*

Cmty. Bank v. Schnuck Mkts., Inc.,
887 F.3d 803 (7th Cir. 2018)..... 22

Dieffenbach v. Barnes & Noble, Inc.,
887 F.3d 826 (7th Cir. 2018)..... 17, 22

Flast v. Cohen,
392 U.S. 83 (1968)..... 19

Friends of the Earth, Inc.
v. Laidlaw Envtl. Servs. (TOC), Inc.,
528 U.S. 167 (2000)..... 19

Galaria v. Nationwide Mutual Ins. Co.,
663 F. App'x 384 (6th Cir. 2016) 16, 17

Gladstone, Realtors v. Vill. of Bellwood,
441 U.S. 91 (1979)..... 20

Hutton v. Nat'l Bd. of Examiners in
Optometry, Inc.,
892 F.3d 613 (4th Cir. 2018..... 15

In re Horizon Healthcare Servs. Inc.
Data Breach Litig.,
846 F.3d 625 (3d Cir. 2017) 17, 18

In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.,
45 F. Supp. 3d 14 (D.D.C. 2014)..... 23, 27

In re SuperValu, Inc.,
870 F.3d 763 (8th Cir. 2017)..... *passim*

Katz v. Pershing, LLC,
672 F.3d 64 (1st Cir. 2012) 15

Khan v. Children's Nat'l Health Sys.,
188 F. Supp. 3d 524 (D. Md. 2016)..... 23

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010)..... 8, 9

Lewert v. P.F. Chang's China Bistro, Inc.,
819 F.3d 963 (7th Cir. 2016)..... 17

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992)..... *passim*

Reilly v. Ceridian Corp.,
664 F.3d 38 (3d Cir. 2011) 18, 24, 26

Remijas v. Neiman Marcus Grp., LLC,
794 F.3d 688 (7th Cir. 2015)..... 10, 17

Simon v. E. Ky. Welfare Rights Org.,
426 U.S. 26 (1976)..... 19

South Dakota v. Wayfair, Inc.,
138 S. Ct. 2080 (2018)..... 29

Spokeo, Inc. v. Robins,
136 S. Ct. 1540 (2016)..... *passim*

Steel Co. v. Citizens for Better Env't,
523 U.S. 83 (1998)..... 19

Strautins v. Trustwave Holdings, Inc.,
27 F. Supp. 3d 871 (N.D. Ill. 2014)..... 23

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014)..... *passim*

Town of Chester v. Laroe Estates, Inc.,
137 S. Ct. 1645 (2017)..... 26

Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.,
454 U.S. 464 (1982)..... 20

Warth v. Seldin,
422 U.S. 490 (1975)..... 19

Whalen v. Michaels Stores, Inc.,
689 F. App'x 89 (2d Cir. 2017)..... 15, 22

Whitmore v. Arkansas,
495 U.S. 149 (1990)..... 20, 21, 24

Constitutional Provisions

U.S. Const. art. III, §§1-2 19

Other Authorities

2017 Data Breaches Hit Half-Year Record High, Identity Theft Resource Ctr.,
https://bit.ly/2yT8Avc
(last visited Aug. 20, 2018)..... 28

Br. in Opp'n, *Carefirst, Inc. v. Attias*,
No. 17-641, 2018 WL 300630
(U.S. Jan. 2, 2018) 31

Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*,
52 Gonz. L. Rev. 59 (2017)..... 28

Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* (Feb. 2018),
https://bit.ly/2KeJyXT 30

Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. Cal. L. Rev. 683 (2017) 1, 28

Edward H. Klees, *The "Fandation" of Risk: Does A Banking Client Get Its Money Back After Cyber Theft?*, Bus. L. Today, May 2016 ..... 1, 28, 29

Mike Murphy, *A new data breach may have exposed personal information of almost every American adult*, MarketWatch (Jun. 28, 2018), https://on.mktw.net/2IC6dfM 29

Kenneth Olmstead & Aaron Smith, Pew Res. Ctr., *Americans & Cybersecurity* (Jan. 2017) 1, 3, 28

Pet. for Writ of Certiorari, *Beck v. Shulkin*, No. 16-1328, 2017 WL 1756935 (U.S. Apr. 27, 2017) 31

Ponemon Inst., *2018 Cost of a Data Breach Study: Global Overview* (July 2018) https://bit.ly/2M7zZPB. 29

PETITION FOR WRIT OF CERTIORARI

In the modern, online world, "hacking attacks are a fact of life." Edward H. Klees, *The "Fandation" of Risk: Does A Banking Client Get Its Money Back After Cyber Theft?*, Bus. L. Today, May 2016, at 1. In 2016, more than 75% of American companies suffered at least one data breach. Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. Cal. L. Rev. 683, 685 (2017). And roughly two-thirds of American adults "have experienced or been notified of a significant data breach pertaining to their personal data or accounts." Kenneth Olmstead & Aaron Smith, Pew Res. Ctr., *Americans & Cybersecurity* at 8, 23 (Jan. 2017). Fortunately, though, not all data breaches are equally harmful. In fact, many (if not most) data breaches result in no concrete harm to affected individuals. If companies design their systems properly, sensitive data cannot be obtained. And if companies respond quickly and appropriately, customers can take additional measures to ensure injuries are prevented. As a result, only a small fraction of recent data breaches have led to any meaningful reports of identity theft or fraud. *See In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017).

For precisely that reason, the First, Second, Fourth, and Eighth Circuits have concluded that plaintiffs cannot establish Article III standing to sue the holder of data subjected to a data breach simply by pointing to the breach itself. In those circuits, the mere possibility that the data will be misused in a manner that inflicts concrete injury does not suffice to satisfy Article III. After all, this Court has made

crystal clear that an injury must be "'actual or imminent, not conjectural or hypothetical,'" to satisfy Article III. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). "An allegation of future injury" thus will suffice to satisfy Article III only if the injury is "certainly impending"—*i.e.*, only if there is "a 'substantial risk that the harm will occur.'" *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). The mere possibility that information stored in a breached database may *someday* be misused is manifestly insufficient to satisfy that standard.

Nonetheless, five other circuits—including the Ninth Circuit in the decision below—have taken the position that plaintiffs satisfy Article III and allege "a credible threat of real and immediate harm" simply by alleging that their information was stored in a breached database, even if they do not and cannot allege that their information has actually been misused in a manner that inflicts concrete injury. App.8. Indeed, in this case, the defendant took immediate steps as soon as it identified the data breach that strictly limited, if not eliminated, the potential for misuse of the data. Yet the Ninth Circuit allowed the plaintiffs' putative class actions to go forward even though the plaintiffs concededly have suffered no misuse of their own data and could identify only two dozen individuals out of a pool of *24 million* who have ever even claimed that their data were misused in the six years since the data breach was detected and addressed. There is thus a clear and acknowledged circuit split over what a plaintiff must

allege to adequately plead Article III standing when suing for damages in response to a data breach.

This Court's intervention is sorely needed. Mere exposure to a data breach is an unfortunate fact of life in our increasingly virtual world. "[T]here is a general public consensus that the coming years will likely see significant attacks on our public infrastructure and financial systems." Olmstead & Smith, *supra*, at 8. But Article III courts exist to redress particularized and concrete injuries, not to address broadly shared risks of potential injury. The expansive view of standing embraced by the Ninth Circuit and four other circuits ignores that fundamental distinction and opens the courts to abstract suits that fail to focus on and compensate concrete injuries. Worse still, by subjecting all manner of retailers, employers, and service providers victimized by a data breach to the prospect of sprawling and costly litigation, no matter how adroitly and effectively they respond, the decision below severely dulls incentives to take immediate steps to prevent actual misuse of the data. The decision below thus not only is wrong, but is of enormous consequence in the Internet age. And this is an ideal case in which to resolve this issue, as it is squarely and cleanly presented. The Court should grant certiorari.

OPINIONS BELOW

The amended opinion of the Ninth Circuit is reported at 888 F.3d 1020 and reproduced at App.1-19. The district court's order granting in part Zappos' motion to dismiss the third amended consolidated class complaint is available at 2016 WL 2637810 and reproduced at App.26-46. The district court's order

granting Zappos' motion to dismiss the second amended class complaints is reported at 108 F. Supp. 3d 949 and reproduced at App.47-72.

JURISDICTION

The Ninth Circuit issued its amended opinion on April 20, 2018. On July 2, 2018, Justice Kennedy extended the time for filing a petition to and including August 20, 2018. This Court has jurisdiction under 28 U.S.C. §1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Article III, §§1-2 of the U.S. Constitution is reproduced at App.73-74.

STATEMENT OF THE CASE

A. Factual Background

Zappos is one of the nation's premier online retailers, which also makes it a target for hackers. Cognizant of that risk, Zappos not only endeavored to secure its systems against a database breach, but also put in place security measures designed to prevent hackers from being able to use data to inflict harm in the event of a breach. For instance, Zappos stored customer password data in a cryptographically scrambled state, kept credit card information in a separate database, and had in place a plan to deal immediately with a breach should one occur. App.47-48, 65-66.

Unfortunately, in January of 2012, Zappos was the victim of a data breach. Hackers breached Zappos' computer systems, including servers that contained the personal identifying information (*i.e.*, names and contact information) of 24 million Zappos customers.

App.26-27. Partial credit card information may also have been accessed, but no respondent has alleged that any fraudulent charges occurred on any of their credit cards. Nor have there been any reports of increased rates of credit card fraud across the population of Zappos customers. App.5.

Fortunately, Zappos responded to the breach swiftly and decisively. Zappos immediately cut access between its systems and the outside world, and immediately suspended all online ordering activity until customers' account passwords could be reset. App.5, 48. Zappos also promptly notified all customers of the incident and specifically advised customers to change their passwords immediately. App.5-6. That swift action prevented the attack from inflicting concrete harm on its customers. Today, more than six years after the incident, only a handful of individuals (none of whom have alleged specific causation) have ever reported concerns that their information may have been misused as a result of the breach. App.31-33, 61-64.

B. Procedural History

1. District Court Proceedings

Zappos' precautionary measures and swift response may have prevented the hackers from misusing customer data, but they did not prevent the inevitable lawsuits. Within days of the breach, several customers filed putative class actions against Zappos in district courts across the country, seeking to represent all 24 million individuals whose data were stored in the breached systems. The Judicial Panel on Multidistrict Litigation (MDL) ultimately transferred

the various cases to the District of Nevada for consolidated pretrial proceedings. *See* Dkt.1.[1]

In November of 2012, two sets of plaintiffs filed two separate amended complaints in the MDL court alleging state-law negligence, contract, and invasion of privacy claims, various state-law statutory claims, and claims under the Fair Credit Reporting Act (FCRA). *See* Dkts.58-59. After the district court dismissed "most of the common law claims," Dkt.114, plaintiffs filed two second amended class complaints realleging nearly all the same claims, Dkts.118-19.

On June 1, 2015, after multiple rounds of briefing on the pleadings, extensive discovery, and an unsuccessful mediation, the district court dismissed all of the plaintiffs' claims with leave to amend. App.47-72. The court concluded that plaintiffs lacked Article III standing because they did not adequately allege that the breach caused, or was imminently likely to cause, them any actual injury. "It is not enough," the court explained, "that a credible threat may occur at some point in the future; rather, the threat must be impending." App.60. Yet notwithstanding the considerable "passage of time" since the breach—by then, nearly three years—plaintiffs alleged no identity theft, data misuse, fraudulent credit card charges, or any other concrete injury from the breach. App.62. The court observed that "[t]he years that have passed without Plaintiffs making a single allegation of theft or fraud demonstrate that the risk is not immediate…. The

[1] All references to "Dkt." are to the docket in Case No. 3:12-cv-00325-RCJ-VPC (D. Nev.), the transferee court in MDL No. 2357.

possibility that the alleged harm could transpire in the as-of-yet undetermined future relegates Plaintiffs' injuries to the realm of speculation." App.63.

Plaintiffs responded to the dismissal by filing a single, consolidated, third amended class complaint. Even in the new complaint, however, plaintiffs still did not allege that they had suffered any fraud or identity theft as a result of the breach. They instead continued to allege only that they "spent time changing" their Zappos passwords and that they lost "the exclusive right to monetize" their personal identifying information. Dkt.245. The new complaint did include allegations from two *new* plaintiffs who claimed to have experienced fraudulent charges as a result of the breach. The new complaint also referenced 22 informal complaints that customers had made to Zappos about the breach, which Zappos had disclosed to plaintiffs in discovery. Dkt.245.

On May 6, 2016, the district court issued an order once again dismissing all of the original plaintiffs' claims, but allowing the claims of the two new plaintiffs who alleged actual fraudulent charges to proceed. The court concluded that the allegations of the two new plaintiffs sufficed for Article III at the pleading stage. App.33-38. But as to the original plaintiffs, the court concluded that they still failed to satisfy Article III, as they did not allege that they personally suffered, or were imminently likely to suffer, any fraud or identity theft. As the court explained, allegations that a mere handful of customers may have suffered some actual injury could not suffice to demonstrate that the other 24 million

affected individuals were facing an imminent risk of concrete harm. App.31-33.

Plaintiffs moved for reconsideration after this Court issued its decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). Dkt.282. The district court denied the motion but made clear that if at some future point the original plaintiffs actually suffered fraud or identity theft as a result of the breach, they could file a new complaint. Dkt.287.

2. The Decision Below

Instead of taking the district court up on its offer to come back if and when any actual injury ever materialized, plaintiffs stipulated to dismiss their claims with prejudice in order to pursue an immediate appeal. Dkt.288. As a result, only the original plaintiffs' claims, *not* the claims of the two new plaintiffs who alleged that they had suffered actual identity theft stemming from the January 2012 data breach, were at issue on appeal. App.7, 14. The Ninth Circuit thus acknowledged that no plaintiff-appellant before it had alleged any actual identity theft or fraud as a result of the data breach. App.13-14. Nonetheless, relying on *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the Ninth Circuit reversed. App.13-17.

Krottner, which was decided before this Court's decision in *Clapper*, is a case in which Starbucks employees sued the company after a computer that contained "the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees" was stolen. 628 F.3d at 1140. As in this case, no plaintiff in *Krottner* alleged that his personal identifying information had actually been

misused after the theft in a manner that inflicted any concrete injury. *Id.* at 1142. Yet the court held that the theft of the laptop *itself* created Article III injury, even in the absence of any allegations that the plaintiffs' data had been misused, because the theft established "a credible threat of real and immediate harm" that the plaintiffs' information *could be* misused sometime in the future. *Id.* at 1143-44.

Zappos argued that *Krottner* had been superseded by *Clapper*, which subsequently held that a future injury must be "certainly impending" to satisfy Article III. But the Ninth Circuit disagreed, instead reading *Clapper* narrowly to apply only when a plaintiff seeks to establish standing based on "a speculative multi-link chain of inferences" to declare unconstitutional "actions of the executive and legislative branches" "in a sensitive national security context." App.11. The Ninth Circuit also drew a purported distinction between *Clapper* and "other cases" that "focused on whether there was a 'substantial risk' of injury," not "whether the injury was 'certainly impending.'" App.11-12 (citing *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014)). Relying on those cases, the Ninth Circuit concluded that *Krottner*—under which Article III is satisfied (at least at the pleading stage) whenever a plaintiff alleges that his "unencrypted personal data" has been stolen, 628 F.3d at 1143—"controls the result here." App.13.

Applying *Krottner*, the court concluded that plaintiffs' allegations that the Zappos data breach "places them at imminent risk of identity theft" suffice for Article III. App.15. The court further concluded that the allegations of the two late-added plaintiffs

(whose "claims are not at issue in this appeal") "undermine[d] Zappos's assertion that the data stolen in the breach cannot be used for fraud or identity theft." App.14. Finally, the court rejected the argument that the passage of time since the data breach undercut the alleged "imminence" of the harm, finding it sufficient that plaintiffs "allege that … 'it may take some time for the victim to become aware of the theft.'" App.16-17.

In so holding, the court acknowledged that the Eighth Circuit has held "that allegations of the theft of credit card information were insufficient to support standing." App.12 n.6; *see In re SuperValu*, 870 F.3d 763. But the court tried to distinguish *In re SuperValu* as turning on "the types of data allegedly stolen." App.12 n.6. The court noted that its opinion "is consistent with post-*Clapper* decisions" from other "circuits holding that data breaches in which hackers targeted [personal identifying information] created a risk of harm sufficient to support standing." *Id.* (citing *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017), and *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)).

Zappos sought rehearing, which was denied, but the petition prompted the panel to issue an amended opinion clarifying that, in its view, both "the original Complaints [and] Plaintiffs' Third Amended Complaint" contain sufficient "allegations about the increased risk of harm Plaintiffs face." App.2. The panel then entered an order staying its mandate "for a period not to exceed 90 days," App.21, and subsequently extended that stay "pending the filing of

[a] petition for a writ of certiorari in the Supreme Court," App.23.

REASONS FOR GRANTING THE PETITION

The decision below deepens an acknowledged circuit split on a recurring and important issue of constitutional law. In four circuits, bare allegations that a database containing a plaintiff's nonpublic personal information has been breached, without specific allegations of resulting misuse of the data and concrete harm, do not suffice for Article III standing. In five circuits, they do, and plaintiffs can pursue sprawling class actions simply by alleging that a database holding their nonpublic personal information was breached. This split is clear, it is acknowledged, and its importance is only increasing. The time has come for this Court to resolve it.

The decision below conflicts not only with decisions from four other circuits, but also with this Court's standing precedent and bedrock principles of Article III. Article III requires a plaintiff to allege concrete harm. When, as here, a plaintiff seeks to establish standing by alleging that he will suffer injury in the future, that injury must be "imminent," *i.e.*, "not conjectural or hypothetical." *Spokeo*, 136 S. Ct. at 1548. As this Court recently reiterated, that means that the injury must be "certainly impending," *Clapper*, 568 U.S. at 401, 410-14—there must be a "substantial risk" that it actually "will occur." *Susan B. Anthony List*, 134 S. Ct. at 2341.

As this case vividly illustrates, the mere fact that a database containing an individual's information has been breached does not make the actual misuse of that information "imminent," "certainly impending," or a

"substantial risk." Indeed, after six years of litigation and discovery, respondents have identified a grand total of (at most) 24 individuals—out of *24 million*—who have ever even claimed that their data might have been misused as a result of the breach. An alleged risk of an injury that still has not materialized more than half a decade after the fact is the very essence of "conjectural or hypothetical." Moreover, the decision below not only is wrong as matter of Article III doctrine, but creates perverse incentives. Companies that plan with foresight and react with dispatch can prevent potential data-breach-related harms from materializing. But if a company that takes decisive action and promptly notifies customers will inevitably face a class action lawsuit even if injuries are averted, the proper incentives for preventing harm will be dulled.

This case is an ideal vehicle to resolve this open and acknowledged circuit split on an important and recurring issue. The sole question at issue on appeal was whether respondents—plaintiffs who concededly did *not* allege that they have suffered any identity theft or fraud—could satisfy Article III by alleging an increased risk of future identity theft stemming from the breach. Indeed, the district court specifically distinguished between the two plaintiffs who actually alleged an injury from data misuse and the plaintiffs (and millions of putative class members) who did not, and only the claims of the latter are at issue in this petition. This case thus presents an excellent opportunity to address an issue of increasing importance.

I. There Is An Acknowledged Split Of Authority On The Question Presented.

Under this Court's precedent, a plaintiff who seeks to establish a concrete Article III injury by alleging some *future* harm must allege an anticipated injury that is "certainly impending." *Clapper*, 568 U.S. at 401, 410-14. As the Fourth Circuit recently observed, the "circuits are divided on" how that standard applies in the context of a data breach. *Beck v. McDonald*, 848 F.3d 262, 273 (4th Cir. 2017). While four circuits have concluded that the mere existence of a data breach does not, in and of itself, suffice to make future injury "certainly impending," the Ninth Circuit and four other circuits have deemed a breach itself sufficient to confer Article III standing to sue the target of the attack. This split is square, it is acknowledged, it has persisted after *Clapper*, and it is deep.

1. On one side of the split, the Eighth Circuit has squarely held that merely alleging a data breach does not suffice to establish Article III standing. *See In re SuperValu*, 870 F.3d at 771. *SuperValu* involved a grocery store chain that "suffered two cyber attacks in which their customers' financial information," including credit card information, "was allegedly accessed and stolen." *Id.* at 765. Sixteen customers who shopped at SuperValu brought suit, seeking to represent a class of all potentially affected customers. While that putative class numbered in the thousands, the plaintiffs did not identify a single plaintiff (themselves included) whose data had been misused in the wake of the breach. Instead, the plaintiffs relied solely on the theory that the breach "create[d] a

substantial risk that they w[ould] suffer identify theft" at some point in the future. *Id.* at 770. After expressly acknowledging a division of authority on the issue, the Eighth Circuit disagreed with the plaintiffs, concluding that "a mere possibility" that identity theft or some other form of data misuse may occur "is not enough for standing." *Id.* at 771. The court further concluded that "the time [plaintiffs allegedly] spent protecting themselves against this speculative threat cannot create an injury" under Article III. *Id.*

The Fourth Circuit reached the same conclusion in *Beck v. McDonald*, holding that a plaintiff cannot "establish Article III standing based on the harm from the increased risk of future identity theft and the cost of measures to protect against" that speculative potential harm. 848 F.3d at 266-67. In *Beck*, thieves stole a laptop and boxes containing patients' personal identifying information, including names, addresses, dates of birth, partial social security numbers, and physical descriptions. Two individuals brought suit, seeking to represent a class of all 7,400 patients whose information was stored in the breached files. As in *SuperValu* and this case, the plaintiffs did not allege that their information (or anyone else's) had been misused or that they had suffered any identity theft or other harm. Instead, they maintained that the security breach itself, and their own actions in the wake of it, sufficed to establish standing. *Id.* at 267.

The Fourth Circuit acknowledged that "[o]ur sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on the increased risk of future identify theft." *Id.* at 273. Siding with the circuits that have answered that

question in the negative, the court concluded that the plaintiffs failed to plead any concrete injury within the meaning of Article III. *Id.* at 274-75. Since then, the Fourth Circuit has reiterated its view that "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018); *see also id.* at 622 ("incurring costs for mitigating measures to safeguard against future identity theft" does not satisfy Article III "when that injury is speculative").

The Second Circuit likewise has held that allegations that a plaintiff "faces a risk of future identity fraud" because her "credit card information was stolen" do not constitute "particularized and concrete injury" under Article III. *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 91-92 (2d Cir. 2017). Like the Fourth and Eighth Circuits, *Whalen* further held that allegations that a plaintiff "lost time and money resolving the attempted fraudulent charges and monitoring her credit" do not suffice for Article III injury, at least when the plaintiff has not had to pay for any fraudulent charges. *Id.* And the First Circuit has said that allegations "that the defendant's failure to adhere to privacy regulations increases her risk of harms associated with the loss of her data" are insufficient to establish Article III injury. *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012).

2. On the other side of the split, five circuits (including the Ninth Circuit in this case) have held that a plaintiff may establish Article III injury by alleging that her nonpublic personal information was

stored in a database that was breached, even if there is no allegation that anyone misused her data.

In *Attias v. Carefirst, Inc.*, the D.C. Circuit confronted a case in which seven individuals sought to bring a putative class action against several health insurance companies after databases containing the plaintiffs' personal information were breached. 865 F.3d at 623-24. Although the plaintiffs did not allege that their information had been misused or that they had suffered any identity theft or fraud as a result of the breach, the court nonetheless held that the mere fact that their information was stored in the breached database created a sufficiently "substantial risk" of future identity theft to satisfy Article III. *Id.* at 627-28. In the D.C. Circuit's view, standing exists because if "an unauthorized party has already accessed personally identifying data" on nonpublic servers, "it is plausible … to infer that this party has both the intent and the ability to use that data for ill." *Id.* at 628.

The Sixth Circuit reached a similar conclusion in *Galaria v. Nationwide Mutual Insurance Co.*, where two individuals sought to represent a million-person class after hackers allegedly breached Nationwide's network and "stole their personal information." 663 F. App'x 384, 385 (6th Cir. 2016). As in *Attias* (and this case), the plaintiffs in *Galaria* did not allege that they (or anyone in the putative class) had actually suffered any identity theft or fraud as a result of the hack. *See id.* at 386-87. The Sixth Circuit nevertheless held that the plaintiffs' allegations "that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft"

sufficed for Article III. *Id.* at 388. According to the Sixth Circuit, such allegations were not unduly speculative because "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for … fraudulent purposes." *Id.*

The Seventh Circuit has repeatedly held "that consumers who experience a theft of their data indeed have standing" regardless of whether they allege any actual identity theft or fraud. *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018); *see Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965-67 (7th Cir. 2016) (allegations that consumers who dined at a restaurant whose "computer system [was] breached" faced an "increased risk of fraudulent charges and identity theft … concrete enough to support a lawsuit"); *Remijas*, 794 F.3d at 693 (allegations that customers' "information ha[d] been stolen" from a department store database created sufficient risk that "identity theft or credit card fraud" "will occur").

And the Third Circuit reached the same result in *In re Horizon Healthcare Services Inc. Data Breach Litigation*, where customers brought a putative class action after two laptops containing unencrypted personal information (including health information) were stolen from Horizon. 846 F.3d 625, 629-30 (3d Cir. 2017). Out of a class of 839,000 Horizon members, only *one* plaintiff alleged that any stolen information was actually used to his detriment. *Id.* at 630 (one plaintiff alleged that, "[a]s a result of the Data Breach," he was "denied retail credit because his social security number has been associated with identity

theft"). The Third Circuit nevertheless held that *all* of the plaintiffs pleaded enough for Article III. *Id.* at 638-39. That holding stands in stark contrast to the Third Circuit's own previous holding that "allegations of an increased risk of identity theft resulting from a security breach are … insufficient to secure standing" where "no evidence suggests that the data has been—or will ever be—misused." *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011).

In sum, the vast majority of circuits have now confronted the question of what a plaintiff must allege to have standing to bring suit against the victim of a data breach. And the nine circuits that have answered that question are divided nearly equally as to how to answer it. This split is square, it is acknowledged, it includes cases decided before and after *Clapper*, and it necessitates this Court's resolution.

II. The Decision Below Cannot Be Reconciled With This Court's Precedent.

The decision below not only parts ways with the decisions of four other circuits, but cannot be reconciled with either this Court's precedents or bedrock principles of Article III. This Court's decision in *Clapper* could not have been clearer that an actual injury must be *imminent*, not just possible, to give rise to Article III standing. As this case vividly illustrates, that standard cannot be satisfied just by alleging that a data breach occurred.

A. Future Injuries Must Be "Certainly Impending" To Satisfy Article III.

Article III of the U.S. Constitution limits the "judicial Power of the United States" to the resolution of "Cases" or "Controversies." U.S. Const. art. III, §§1-

2. That limitation is of surpassing importance. "[T]he law of Art. III standing is built on a single basic idea—the idea of separation of powers," *i.e.*, limiting courts to their proper sphere. *Allen v. Wright*, 468 U.S. 737, 752 (1984). "No principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 37 (1976); *see Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 191 (2000) (standing doctrine "functions to ensure … that the scarce resources of the federal courts are devoted to those disputes in which the parties have a concrete stake").

The standing inquiry therefore "focuses on the party seeking to get his complaint before a federal court and not on the issues he wishes to have adjudicated." *Flast v. Cohen*, 392 U.S. 83, 99 (1968). To bring suit in federal court, a plaintiff must prove that he "(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; *see Lujan*, 504 U.S. at 561 ("The party invoking federal jurisdiction bears the burden of establishing these elements."). All three elements of standing are constitutionally compelled, *see id.* at 560-61, but the injury-in-fact requirement is "[f]irst and foremost" among them, *Steel Co. v. Citizens for Better Env't*, 523 U.S. 83, 103 (1998), as it "helps to ensure that the plaintiff has a 'personal stake in the outcome of the controversy,'" *Susan B. Anthony List*, 134 S. Ct. at 2341 (quoting *Warth v. Seldin*, 422 U.S. 490, 498 (1975)). Accordingly, "neither the counsels of

prudence nor the policies implicit" in this Court's justiciability cases can "substitute for a demonstration of 'distinct and palpable injury.'" *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 475 (1982) (quoting *Gladstone, Realtors v. Vill. of Bellwood*, 441 U.S. 91, 100 (1979)).

To satisfy the injury-in-fact requirement, an injury must be more than just "distinct and palpable." An injury must also be "particularized," *i.e.*, it "must affect the plaintiff in a personal and individual way." *Lujan*, 504 U.S. at 560 n.1. And an injury must be "concrete," *i.e.*, "it must actually exist." *Spokeo*, 136 S. Ct. at 1548; *see id.* at 1549 ("Article III standing requires a concrete injury even in the context of a statutory violation."). That is not to say that allegations of future injury can never suffice to state a concrete injury. To the contrary, a "risk of real harm can[] satisfy the requirement of concreteness." *Id.* But an alleged injury "must be concrete in both a qualitative and temporal sense" to satisfy Article III. *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990). Thus, when a plaintiff seeks to sue based on an injury that has not yet materialized (as opposed to an injury that has already taken place), the alleged injury cannot be "conjectural or hypothetical"; it must be "imminent." *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560).

"Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." *Clapper*, 568 U.S. at

409 (quoting *Lujan*, 555 U.S. at 565 n.2). "Allegations of *possible* future injury" therefore "do not satisfy the requirements of Art. III." *Whitmore*, 495 U.S. at 158 (emphasis added). Instead, there must be at least "a 'substantial' risk that the harm will occur." *Susan B. Anthony List*, 134 S. Ct. at 2341 (quoting *Clapper*, 568 U.S. at 414 n.5).

B. Respondents Did Not Allege Substantial Risk That Harm Will Occur.

The decision below cannot be reconciled with that settled law, as a data breach alone simply does not make any potential injury resulting from that breach "*certainly* impending." *See Clapper*, 568 U.S. at 409. Instead, the prospect that information stored in a breached database might subsequently be put to misuse by the perpetrator of the attack is a classic example of a "conjectural or hypothetical" injury. *See Lujan*, 504 U.S. at 560.

This is a case in point. The Zappos database that hackers breached in January of 2012 contained the names and contact information of roughly 24 million customers. Of those 24 million customers, respondents have managed to identify a grand total of 24—0.00001%—who have ever even claimed that their information was misused as a result of the breach. And that is after six years of litigation and extensive discovery, no less. Respondents themselves have not "detected any irregularity whatsoever in regards to unauthorized purchases or other manifestations that their personal information has been misused," App.61, and they came up with only two plaintiffs who were able to allege otherwise, *see* App.33-35. That should come as little surprise. Even assuming the

perpetrators of the 2012 attack intended to put customers' data to misuse, Zappos never held extremely sensitive information like social security numbers or medical information; Zappos employed sophisticated cryptological techniques to prevent effective use of password data in the event of a breach; Zappos kept credit card information in a separate database altogether; Zappos quickly detected the January 2012 breach; and Zappos promptly notified customers of the breach, thereby halting any imminent risk of harm.[2]

Respondents' inability to allege any actual injury in the six-plus years of this litigation is not for lack of trying. The district court gave them every opportunity. Respondents took discovery, plumbing the online depths of their own personal information and combing through reams of documents and data that Zappos disclosed. Yet for all of their searching,

---

[2] Even if respondents *had* suffered some credit irregularities or fraudulent charges—which they have not—it still would have been highly unlikely that respondents themselves would have been forced to bear the financial consequences. Existing contractual arrangements among retailers, credit card issuers, and credit card processing networks typically allocate among themselves the costs associated with protecting customers/cardholders from unauthorized charges, *i.e.*, they shield the customers/cardholders from the cost. *See Cmty. Bank v. Schnuck Mkts., Inc.*, 887 F.3d 803, 808-09 (7th Cir. 2018). Thus, even in the rare cases in which a breach *does* result in actual fraud, cardholders will rarely, if ever, be forced to foot the bill. *See, e.g.*, *Whalen*, 689 F. App'x at 90 (no standing where prompt cancellation of credit card prevented any harm befalling cardholder). *But see Dieffenbach*, 887 F.3d at 828 ("unauthorized withdrawals from [plaintiffs'] accounts cause a loss (the time value of money)" sufficient for Article III standing).

respondents found only 22 informal complaints made to Zappos about the breach, and identified only two plaintiffs to claim their data were actually misused. *See* Dkt.245 ¶67. In other words, respondents found no basis on which to claim actual or imminent concrete harm either to themselves or to the 24 million putative class members they seek to represent.

That makes the decision below (and the decisions of other circuits embracing the same reasoning) impossible to reconcile with this Court's precedents. As *Clapper* made crystal clear, future injury must be "*certainly* impending" to satisfy Article III. 568 U.S. at 401, 409-14. Indeed, even an "objectively reasonable likelihood" of future injury is not enough, as that does not make an injury *imminent*. *Id.* at 410. As one lower court thus aptly put it, "*Clapper* seems rather plainly to reject the premise … that any marginal increase in risk [of future injury] is sufficient to confer standing." *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 878 (N.D. Ill. 2014); *see, e.g.*, *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533 (D. Md. 2016) ("general allegations … that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft" insufficient); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (no "substantial risk" of harm where "[b]y Plaintiff's own calculations … injury is likely not impending for over 80% of victims"). And the "certainly impending" standard *Clapper* invoked is by no means unique to the "national security context," App.11, but rather can be found in Article III cases arising in all manner of

contexts. *See, e.g.*, *Lujan*, 504 U.S. at 564 n.2; *Whitmore*, 495 U.S. at 158.

Clapper also forecloses respondents' effort to manufacture standing by pointing to time or money they chose to spend monitoring their financial information following the breach. The plaintiffs in *Clapper* likewise alleged "that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations … or to travel so that they can have in-person conversations." *Clapper*, 568 U.S. at 415. But that did not cure the problem that "the harm" they spent time and money seeking to avoid was speculative, "not certainly impending." *Id.* at 416. As the Court put it, plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Id.* So too here. Respondents' alleged financial-monitoring expenditures "do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for [their] claims." *Reilly*, 664 F.3d at 46. Any other conclusion would allow respondents to generate their own standing and be "tantamount to accepting a repackaged version of [the] failed theory" that the hypothetical future injury is imminent. *Clapper*, 568 U.S. at 416.

The Ninth Circuit was equally wrong in its attempt to find daylight between *Clapper* and *Susan B. Anthony List*. *See* App.11-12. Invoking *Susan B. Anthony List*, the Ninth Circuit perceived a purported distinction between injuries that are "certainly

impending" and injuries with a "substantial risk [that they] … will occur." App.12 (quoting *Susan B. Anthony List*, 134 S. Ct. at 2341). That is a distinction without a difference. Where there is "a 'substantial risk' that the harm will occur," that harm *is* "certainly impending." *Clapper*, 568 U.S. at 414 n.5. They are simply two different ways of saying the same thing.

In all events, "to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement," *id.*, respondents still fall far short, as the kinds of allegations on which they rely are nothing like the allegations in *Susan B. Anthony List*. There, the plaintiffs alleged that the Ohio Election Commission would bring civil and criminal proceedings against them based on their planned exercise of free speech. *Susan B. Anthony List*, 134 S. Ct. at 2346. That was no mere speculation: The same Commission had already taken action against one of them for similar speech in the past, and there was "every reason to think that similar speech in the future will result in similar proceedings." *Id.* at 2345. Here, in contrast, *no* respondent has alleged *any* identity theft or fraud stemming from the breach. And as explained above, many, indeed most, data breaches do not result in any fraud or identity theft. Accordingly, all respondents have to go on is "speculation about 'the unfettered choices made by independent actors not before the court,'" namely, the individual (or individuals) responsible for the January 2012 data breach. *Clapper*, 568 U.S. at 414 n.5 (quoting *Lujan*, 504 U.S. at 562). That is manifestly not enough.

Nor may respondents bootstrap their way into Article III by pointing to *other* individuals' purported injuries. This is not an injunctive relief suit; it is a damages suit. And in a suit for damages, this Court's case law is clear: *All* plaintiffs seeking damages in federal court must demonstrate their own Article III injury in fact; pointing to injuries sustained by other plaintiffs does not suffice. *Town of Chester v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650-51 (2017); *see Spokeo*, 136 S. Ct. at 1547 n.6 ("named plaintiffs who represent a class must allege and show that they *personally* have been injured, not that injury has been suffered by other … members of the class to which they belong" (emphasis added)); *In re SuperValu*, 870 F.3d at 771 (affirming dismissal of all but one plaintiff despite that plaintiff's allegation of actual identity theft).

The increased-likelihood theory embraced below fails here for yet another reason: the passage of time. Hackers seeking protected data for financial gain do not typically hold onto data for years before attempting to monetize it. Thus, as "breaches fade further into the past, the … threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275. Here, more than six years have passed, and only an infinitesimally small number of potentially affected individuals have *ever* claimed that any data misuse may have resulted. That just goes to show how truly speculative respondents' claims are, as they allege only "mere conjecture about possible" harm by third parties that six-plus years have shown is unlikely to materialize (let alone do so imminently). *Clapper*, 568 U.S. at 420; *see also Reilly*, 664 F.3d at 45 (any potential future damages "are entirely

speculative and dependent on the skill and intent of the hacker"); *In re SAIC Backup Tape Data Theft Litig.*, 45 F. Supp. 3d at 25 (odds of actual harm are "entirely dependent on the actions of an unknown third party—namely, the thief").

Finally, the decision below is inconsistent with bedrock principles of Article III. The requirement of a concrete, non-speculative injury ensures that Article III courts focus on redressing real injuries and resolving actual disputes. Relaxing that requirement to address potential injuries that may or may not materialize risks having courts adjudicate hypothetical questions for massive numbers of people. That phenomenon not only diverts scarce judicial resources, but also forces courts to adjudicate disputes that lack the concreteness on which the proper judicial role depends. That is a particular problem in the context of data breaches, where the defendant was often the direct victim of a hack or theft. In such circumstances, it is difficult for courts to determine whether the defendant took sufficient precautions or adequate responsive actions without knowing whether any customers' data were actually misused for identity theft or fraud. And the Ninth Circuit's rule creates perverse incentives by failing to distinguish cases where a hacked company failed to take adequate precautions or delayed in its response from those where the victimized company took decisive actions to prevent its customers from becoming victims. In short, the decision below conflicts with this Court's precedents, with the fundamental Article III principles that those decisions reflect, and with common sense.

III. This Case Is An Ideal Vehicle To Resolve The Split On This Frequently Recurring And Exceedingly Important Issue.

The question presented in this case is a recurring issue of substantial and nationwide importance. "Cyberattacks that cause widespread data breaches are more prevalent now than ever before." Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 Gonz. L. Rev. 59, 60 (2017). The facts are staggering. In 2016, more than 75% of American companies suffered at least one data breach. Dowty, *supra*, at 685. And roughly two-thirds of American adults "have experienced or been notified of a significant data breach pertaining to their personal data or accounts." Olmstead & Smith, *supra*, at 8. Add it all up, and it is clear that "hacking attacks are a fact of life" in the modern, online world. Klees, *supra*, at 1.

That trend is not likely to abate anytime soon. Despite increased awareness of and efforts to quell the threat hackers pose to online systems, "data breaches have continued to set new records" almost every year for the past decade "for both the number of events and the numbers of compromised consumer records." *2017 Data Breaches Hit Half-Year Record High*, Identity Theft Resource Ctr., https://bit.ly/2yT8Avc (last visited Aug. 20, 2018). In fact, experts expect that more than one-quarter of *all* companies doing business in the United States will experience a "material" breach at some point in just the next two years. *See* Ponemon Inst., *2018 Cost of a Data Breach Study: Global Overview* 3 & n.3 (July 2018),

https://bit.ly/2M7zZPB.[3] And the explosive growth of e-commerce guarantees that the problem will only get worse. *See South Dakota v. Wayfair, Inc.*, 138 S. Ct. 2080, 2097 (2018) (in 2017, "e-commerce grew at four times the rate of traditional retail, and it shows no sign of any slower pace"). More e-commerce means more businesses operating online; more businesses operating online means more businesses holding more individuals' personal information online; and more personal information online in turn creates more and more temptation for digital ne'er-do-wells with myriad motivations.[4]

Fortunately, while the many businesses, employers, and other organizations that store data online might not be able to stop hacks from happening, they are increasingly able to prevent hackers from misusing any data that hackers might unlawfully access. "As hacking techniques evolve, antihacking vendors release new software to overcome them …." Klees, *supra*, at 1. Moreover, data breaches are increasingly the work of nation-states, "hacktivists," and other actors not primarily motivated by personal financial gain. *See* Council of Economic Advisers, *The*

---

[3] The report defines a "material" breach as an event involving at least 1,000 lost or stolen records.

[4] For instance, reports recently surfaced that a Florida-based data aggregation company "may have exposed the personal data of nearly every American adult." Mike Murphy, *A new data breach may have exposed personal information of almost every American adult*, MarketWatch (Jun. 28, 2018), https://on.mktw.net/2IC6dfM. According to one security researcher, the breach exposed the "records of 230 million consumers and 110 million businesses"—"pretty much every U.S. citizen." *Id.*

Cost of Malicious Cyber Activity to the U.S. Economy 3-4 (Feb. 2018), https://bit.ly/2KeJyXT. Accordingly, as a practical matter, the factual scenario this case presents—a database holding customers' personal information is accessed, but virtually no identity theft or fraud results—is an increasingly common one. The widening gap between the number of data breaches and the number of data breaches that result in actual fraud or identity theft only highlights the anomaly that, in five of the nine circuits that have addressed this issue, the reality that a breach is unlikely to result in any actual data misuse is not enough to protect the target of the breach from sprawling and costly class action litigation.

That gap also makes decisions like the Ninth Circuit's decision in this case an enormous problem for anyone who stores any data (which is to say nearly every large organization). If individuals really can bring suit—and do so on behalf of massive classes—simply because a data breach occurred, then every company that suffers a data breach will have to fight on two fronts, devoting massive resources first to preventing and responding to hacks, and then to responding to the inevitable lawsuits seeking treble and punitive damages on behalf of massive classes. Indeed, under the Ninth Circuit's rule, it does not matter how effective a company was at containing a breach and preventing its customers from actual harm; the company can still be sued simply for failing to prevent the nearly inevitable breach. This is a case in point: Zappos has been embroiled in costly MDL and putative class action litigation over the 2012 data breach *for six years*, even though only two dozen of the 24 million potentially affected individuals have ever

even claimed that the breach might have caused them any actual injury. If even that level of success in containing the impact of a breach cannot stop courts from proceeding on the assumption that everyone whose data were stored in a breached database faces "imminent" identity theft or fraud, then the incentives to take immediate steps to prevent actual misuse of the data will be dulled.

Finally, this case is an ideal vehicle to resolve the question presented. After years of discovery and briefing, respondents declined to take the district court up on its offer to bring suit again if and when their claims of future injury ever materialized, and the only plaintiffs who alleged actual harm stipulated to dismissal with prejudice to facilitate the original plaintiffs' appellate review. *See supra* 8. As a result, the claims of the two late-added plaintiffs who *did* allege that they suffered actual identity theft stemming from the breach were not at issue on appeal. App.7; *see* App.14 ("those plaintiffs' claims are not at issue in this appeal"). Thus, the sole issue decided by the Ninth Circuit was whether plaintiffs who concededly did not allege any identity theft or fraud nonetheless adequately alleged Article III standing. That was not true of either of the previous petitions to present this question. *See* Br. in Opp'n at 23-27, *Carefirst, Inc. v. Attias*, No. 17-641, 2018 WL 300630 (U.S. Jan. 2, 2018) ("respondent has also alleged injury in fact based upon actual injury already sustained") (capitalization omitted); Pet. for Writ of Certiorari at 22-23, *Beck v. Shulkin*, No. 16-1328, 2017 WL 1756935 (U.S. Apr. 27, 2017) (emphasizing question of "when historical noncompliance with statute by a government agency is sufficient to show

that a case or controversy exists"). This case thus presents an excellent vehicle for resolving the deep and acknowledged circuit split over what a plaintiff must allege to have standing to sue the victim of a data breach.

CONCLUSION

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

Respectfully submitted,

STEPHEN J. NEWMAN	PAUL D. CLEMENT
JULIA B. STRICKLAND	*Counsel of Record*
BRIAN C. FRONTINO	ERIN E. MURPHY
BRENDAN S. EVERMAN	MATTHEW D. ROWEN
STROOCK & STROOCK & LAVAN LLP	KIRKLAND & ELLIS LLP
2029 Century Park East	655 Fifteenth Street, NW
Suite 1800	Washington, DC 20005
Los Angeles, CA 90067	(202) 879-5000
	paul.clement@kirkland.com

Counsel for Petitioner

August 20, 2018