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 PREIRA, KATHRYN VORHOFF, DENISE RELETHFORD, AND ROBERT REE,

Respondents.

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

BRIEF IN OPPOSITION

Gregory D. Blankinship
Jeremiah Frei-Pearson
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
445 Hamilton Ave.
Suite 605
White Plains, NY 10601

Marc L. Godino
GLANCY, PRONGAY & MURRAY, LLP
1925 Century Park East
Suite 2100
Los Angeles, CA 90067

Ben Barnow
Counsel of Record
Erich P. Schork
BARNOW & ASSOCIATES, P.C.
1 N. LaSalle St., Suite 4600
Chicago, IL 60602
(312) 621-2000
b.barnow@barnowlaw.com

Richard L. Coffman
THE COFFMAN LAW FIRM
505 Orleans St., Fifth Floor
Beaumont, TX 77701

David C. O'Mara
THE O'MARA LAW FIRM, P.C.
311 E. Liberty St.
Reno, NV 89501

QUESTION PRESENTED

A company negligently allowed hackers to obtain customers' names, credit card information, billing addresses, email addresses, and passwords after falsely guaranteeing that it would secure the information. Following the theft, cybercriminals used the stolen information to commandeer email accounts, open unauthorized accounts, and generate fraudulent charges. The question presented is:

Whether the court of appeals correctly determined that victims of the data breach plausibly pleaded a substantial risk of future harm.

PARTIES TO THE PROCEEDING

Petitioner, defendant in the district court and appellee below, is Zappos.com, Inc.

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Authorities

Statutes

Other Authorities

INTRODUCTION

In their complaint, respondents alleged that Zappos.com's use of unsecured servers allowed hackers to obtain numerous customers' sensitive personal information. Hackers used the information to commandeer email accounts, deceptively solicit additional personal data from victims, and rack up fraudulent charges. Respondents, victims of the breach, sued.

Every court of appeals would determine whether respondents alleged an injury-in-fact by applying the same fact-bound legal standard. That standard requires plaintiffs to plausibly allege a substantial risk of future harm, and its application necessarily depends on the facts of each case.

Petitioner mistakes the lower courts' applications of that single, fact-bound standard for legal disagreement. But different outcomes in data breach cases reflect the fact that there are many different kinds of data breaches, and different data breaches give rise to different risks of harm. Deciding whether this particular data breach puts victims at a substantial risk of harm will not help other courts determine whether other data breaches put victims at a substantial risk of harm. And petitioner's decision to improperly dispute the facts alleged in the complaint and attempt to write off respondents' allegations of misuse in various ways would complicate this Court's review of this case.

There is no legal question for this Court to resolve, and it should deny the petition for a writ of certiorari.

STATEMENT OF THE CASE

A. Factual background

Data breaches

"[D]ata breaches are not all alike." Identity Theft Res. Ctr., *2017 Annual Data Breach Year-End Review* 19 (2018), http://bitly.com/2s3TGM9. They "can be broken down into a number of additional sub-categories by what happened and what information (data) was exposed." *Id.*

1. Different data breaches expose different kinds of data, including personally identifiable information ("PII"). PII compromised in a breach can include names, addresses, email addresses, birthdates, places of birth, and biometric data. Nat'l Inst. of Standards & Tech., *Guide to Protecting the Confidentiality of Personally Identifiable Information* ES-1 (2010), https://bit.ly/2AfmwhJ. PII also encompasses government-issued identifiers such as social security, driver's license, and passport numbers. *Id.* And it includes financial account numbers, passwords, credit card numbers, and medical records. *See id.* at ES-1, B-4.

Breaches also differ widely with respect to how the compromised data is stored. For example, data can be encrypted, and "some forms of encryption are more effective than others." U.S. Gov't Accountability Office, GAO-07-737, *Personal Information* 30-31 (2007), https://bit.ly/2Oe7YTh. Additionally, "[d]ata that can only be accessed using specialized equipment and software may be less likely to be misused in the case of a breach." *Id.*

2. Data can be exposed in various ways. For instance, databases can be hacked. And "hacking"

includes "subcategories of phishing, ransomware/malware[,] and skimming." Identity Theft Res. Ctr., *supra*, at 4. Other breaches stem from "unauthorized access," "insider theft," accidental exposure, employee error, "improper disposal," loss, and physical theft. *Id.*

The "method of exposure is a critical category when determining the level of harm potentially associated with a data breach." Identity Theft Res. Ctr., *supra*, at 4. For example, intentional breaches, like hacking, "pose more risk than accidental breaches such as a lost laptop or the unintentional exposure of sensitive data." U.S. Gov't Accountability Office, *supra*, at 30-31.

3. Data breaches can lead to many different forms of misuse. Fraudsters can use PII for the "unauthorized creation of new accounts—such as using someone else's identity to open credit card or bank accounts, originate home mortgages, file tax returns, or apply for government benefits." U.S. Gov't Accountability Office, *supra*, at 30. Other forms of exploitation include "medical identity theft," which involves receiving the victim's health insurance benefits. *Identity Theft*, USA.gov, https://www.usa.gov/identity-theft (last updated Sept. 17, 2018).

Thieves may also misuse victims' existing financial accounts, such as by using payment card information to rack up fraudulent charges. U.S. Gov't Accountability Office, *supra*, at 30. And "even the exposure of emails, passwords[,] or user names can be problematic as this information often plays a role in hacking and phishing attacks." Identity Theft Res. Ctr., *supra*, at 5. PII can also be combined from

multiple sources to create a "mosaic of information" about an individual to enable more fraud. Fed. Chief Info. Officers Council, *Recommendations for Standardized Implementation of Digital Privacy Controls* 7 (2012), https://bit.ly/2SwGSKw. And, as "technology advances," fraudsters can "link information to an individual in ways that were not previously possible." *Id.*

Different types of misuse materialize at different times. Compromised social security numbers and birthdates are "perpetually valuable" and can be "used for years." Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA Today (Sept. 9, 2017), https://bit.ly/2gRLD32. And "child ID theft" can "go undetected for many years." *Identity Theft*, USA.gov, *supra*.

The Zappos.com data breach

The facts about this data breach must be taken from the complaint because this case arises at the pleading stage, at which point respondents' plausible factual allegations are taken as true. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007).

1. Zappos.com, an Amazon subsidiary, is an online retailer that obtained customers' PII in the course of business. Plaintiffs' Third Amended Consolidated Class Action Complaint ¶ 2, ECF No. 245 [hereinafter Compl.]. Zappos.com used the PII for transactions, advertising, and market research. Defendant's Motion to Dismiss Ex. C, at 2-4, ECF No. 62-3. With its "Safe Shopping Guarantee," Zappos.com promised customers that their information would be "absolutely safe." Compl. ¶¶ 59, 167. And customers entrusted Zappos.com with their names, email addresses,

passwords, addresses, credit and debit card information, and telephone numbers. Pet. App. 5.

Zappos.com held this PII in a system that contained unprotected servers, lacked sufficient firewalls, did not properly encrypt the PII, and fell below industry-recommended security standards. Compl. ¶¶ 63-64. Sometime before January 16, 2012, these vulnerabilities allowed hackers to obtain PII of numerous customers, including respondents. *Id.* ¶ 62. Respondents are consumers who purchased shoes and other merchandise from Zappos.com. *Id.* ¶ 2.

Zappos.com first announced its security failure through a brief email notifying customers only that some of their PII "may have been" illegally accessed. Compl. ¶ 62. Zappos.com then shut down its customer-service telephone lines for the week following the breach. *Id.* ¶ 4.

2. Victims learned more about the extent of the breach when fraudsters began exploiting the PII that Zappos.com stored. Respondent Patti Hasner's email account, which used the same username and password as her Zappos.com account, was compromised. Compl. ¶ 34. Zetha Nobles's email account was also exploited. *Id.* ¶ 39-40. Hackers accessed Hasner and Nobles's email accounts and sent fraudulent emails to their contacts. *Id.* ¶¶ 34, 39-40. Additionally, someone used Kristin O'Brien's PII to fraudulently purchase phones, open a credit account at RadioShack, and generate hundreds of dollars in charges. *Id.* ¶ 43. Fraudsters also emptied and overdrew Terri Wadsworth's debit account, and they ran up a $1000 balance on her online

payment account (PayPal), which led eBay to freeze her seller account. *Id.* ¶ 48.[1]

More victims reported similar fraudulent transactions, compromised accounts, and follow-on phishing attempts. Compl. ¶ 67. These alleged incidents of misuse were possible because hackers obtained passwords and full credit and debit card information. *See id.* ¶¶ 34, 39-40, 43, 48, 67.

B. Procedural background

District court proceedings

1. Victims of the Zappos.com data breach filed putative class actions in federal court. In June 2012, several of these cases were consolidated and transferred to the District of Nevada. ECF No. 1. Two consolidated class-action complaints alleged that Zappos.com failed to adequately protect respondents' PII in violation of both common-law rules and statutory provisions. ECF No. 58; ECF No. 59.

Respondents' attempts to obtain discovery did little to develop a full picture of the breach. A year into the litigation, and after an extension for initial disclosures (Order 2, Jan. 10, 2012, ECF No. 81), petitioner had identified only one employee with any knowledge of relevant facts and had produced no documents besides plaintiffs' account histories (Frei-Pearson Declaration Ex. 1, at 4-5, ECF No. 95-1). The magistrate judge accordingly chastised petitioner for its "disappointing" and "unbelievable" refusal to meet court-ordered discovery obligations. Transcript of Motion Hearing 24:1-15, May 7, 2013, ECF No. 109. As

---

[1] O'Brien and Wadsworth were named plaintiffs below. Pet. App. 1, 33.

the magistrate put it, petitioner "very politely listened to my order and then just ignored it." *Id.* 18:1-4

While the magistrate attempted to prod petitioner along, the district court denied in part petitioner's pending motion to dismiss for lack of standing, which argued that respondents had not sufficiently alleged an injury-in-fact in the complaints. Order 5, Sept. 9, 2013, ECF No. 114.[2] The court held that respondents plausibly pleaded injury-in-fact. *Id.*[3]

2. Respondents subsequently filed two amended consolidated complaints. ECF No. 118; ECF No. 119. At that point, the magistrate renewed her concern that the parties were not making "a lot of progress" because of petitioner's "unacceptable" conduct. Transcript of Motion Hearing 5:3-5, 15:9-16:7, Apr. 21, 2014, ECF No. 174. The magistrate had formed the "very disturbing impression" that petitioner possessed "a lack of respect and a disregard for the rules of the [c]ourt and the [c]ourt's orders." *Id.* 62:1-25. For example, Zappos.com produced a "substantial amount" of post-breach customer complaints as "completely redacted, black pages." *See* Compl. ¶ 67 n.3.

Discovery halted for nearly six months after ongoing mediation led to several stays. ECF No. 193; ECF No. 197; ECF. No. 205. But settlement

---

[2] The court explained that "[a]s a general matter . . . [respondents] have standing," but some individual respondents "from Texas, Florida, and Alabama" lacked standing to assert certain "violations of California statutes." Order 5, Sept. 9, 2013, ECF No. 114.

[3] The court dismissed respondents' Fair Credit Reporting Act claim for failure to state a claim. *Id.*

negotiations failed[4] and petitioner soon re-filed its motion to dismiss, arguing again that even if all of respondents' allegations were true, they still would not satisfy Article III. ECF No. 217.

This time, the district court held that respondents had not sufficiently pleaded injury-in-fact. Pet. App. 47. Although the court was addressing a motion to dismiss, it relied on petitioner's representation that no passwords or full credit card numbers were compromised, contrary to the allegations in the complaint. *Id.* 53-67. And it dismissed respondents' claims without prejudice. *Id.* 71.

3. In September 2015, respondents filed their third amended consolidated complaint—the operative complaint. Compl. 76. This complaint included plaintiffs' prior allegations, as well as O'Brien and Wadsworth's allegations of financial loss and twenty-seven complaints lodged with Zappos.com customer service. *Id.* ¶¶ 42-49, 67.

In May 2016, the district court held that O'Brien and Wadsworth had standing but dismissed respondents' claims for lack of standing. Pet. App. 31-38. The parties then stipulated to voluntary dismissal of O'Brien and Wadsworth's claims to facilitate a prompt appeal. *Id.* 24-25.

The decision below

1. The court of appeals reversed. It rejected petitioner's attempts to dispute the facts alleged in the complaint, including that hackers obtained full credit

---

[4] Respondents later claimed that petitioner terminated the negotiations in bad faith and breached a settlement agreement. Compl. ¶¶ 185, 200.

card information, given that petitioner had filed a motion to dismiss. Pet. App. 5 n.2. At this stage, the court explained, plausible allegations must be taken as true. *Id.* The court also explained why the allegations in the complaint were plausible: Allegations that O'Brien and Wadsworth incurred financial losses "undermine[d]" petitioner's counter-assertion that the "data stolen in the breach cannot be used for fraud or identity theft." *Id.* 14.[5]

The court likewise denied petitioner's attempt to "rely[] on facts outside the [c]omplaints" to challenge the plausibility of respondents' allegations. Pet. App. 15-16. Although that maneuver "may be appropriate for summary judgment," it was inappropriate in a motion to dismiss. *Id.* 16.

2. The Ninth Circuit 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." Pet. App. 16-17.

The court recognized that Article III requires plaintiffs to establish a "concrete and particularized" injury-in-fact that is "actual or imminent." Pet. App. 7 (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000)). To satisfy Article III, it explained, future injury must be "certainly impending" or carry a "substantial risk" of occurring. *Id.* 8 (quoting *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014)).

---

[5] The court acknowledged that O'Brien and Wadsworth were "not at issue" in the appeal as individual plaintiffs, Pet. App. 14, because the district court did not dismiss their claims for lack of standing, *id.* 38.

Applying these settled principles, the court concluded that respondents' allegations "adequately alleged an injury in fact supporting standing" given the "sensitivity of the stolen data." *See* Pet. App. 13. Victims' compromised data could "be used to commit identity theft, including by placing them at higher risk of 'phishing' and 'pharming.'" *Id.* Hasner and Nobles's compromised email accounts "further support[ed]" this conclusion, *id.* 14, as did customer reports of fraudulent transactions and other irregularities, *id.* 13 & n.7.

3. Petitioner requested rehearing and argued—for the first time in writing—that the passage of time between the complaints cut against the plausibility of respondents' allegations. *See* Pet. App. 15. The court amended its opinion to acknowledge that petitioner floated this suggestion at oral argument, *id.* 5, 15, but denied rehearing because petitioner provided only "unconvincing" cases to support it, *id.* 15 n.10. No judge on the court of appeals "requested a vote on whether to rehear the matter en banc." *Id.* 3.

REASONS FOR DENYING THE WRIT

I. There is no disagreement among the courts of appeals.

A. The courts of appeals all apply the same fact-bound legal standard.

1. All courts of appeals apply the same legal standard for assessing injury-in-fact. That standard recognizes that an "allegation of future injury" satisfies Article III 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)) (quotation marks omitted). Plaintiffs are not required to "demonstrate that it is literally certain that the harms they identify will come about." *Clapper*, 568 U.S. at 414 n.5.

2. The application of this legal standard necessarily turns on the facts of each case, as different kinds of data breaches give rise to different risks of harm. As petitioner recognized in the court of appeals, decisions in data breach cases "depend heavily on their particular and unique facts, including the nature and seriousness of the breach, [and] the types of information obtained." Def. C.A. Br. 25.

Courts on both sides of petitioner's supposed circuit split agree. The Eighth Circuit explained that courts' standing decisions "ultimately turn[] on the substance of the allegations" before them. *In re SuperValu, Inc.*, 870 F.3d 763, 769 (8th Cir. 2017). The D.C. Circuit also emphasized that decisions like these turn on whether the "specific allegations in the complaint" plausibly establish a "substantial risk of identity fraud." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

District courts similarly understand that the standing analysis is highly fact-specific. *See, e.g.*, *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017) ("Whether the risk of identity theft is sufficiently material to create an injury in fact is 'a question for lower courts to determine in the first instance, on a case- and fact-specific basis.'" (quoting *Katz v. Donna Karan Co.*, 872 F.3d 114, 121 (2d Cir. 2017))); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *3 (S.D. Cal. Nov. 3, 2016) ("Injury-in-

fact analysis is highly case-specific. This is particularly true in the context of data breach.").

3. Because the courts of appeals all use the same fact-bound legal standard, their decisions regularly rely on cases from other circuits.

Decisions from the Second, Fourth, and Eighth Circuits rely on cases from the Sixth, Seventh, and Ninth Circuits. The Second Circuit explained the result in *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89 (2d Cir. 2017), by distinguishing cases from the Sixth and Seventh Circuits. *Id.* at 90-91, 91 n.1. The Fourth Circuit justified its holding in *Beck v. McDonald*, 848 F.3d 262 (4th Cir.), *cert. denied*, 137 S. Ct. 2307 (2017), by explaining how the allegations in Sixth, Seventh, and Ninth Circuit cases "sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274.[6] The Eighth Circuit similarly cited a Seventh Circuit decision recognizing standing as an example of when plaintiffs in the Eighth Circuit could also have standing. *SuperValu,* 870 F.3d at 770-71 (citing *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 692-93 (7th Cir. 2015)).

The same is true of decisions from the other courts of appeals. Decisions from the Sixth and Ninth Circuits rely on decisions from the Fourth and Eighth Circuits. The Sixth Circuit described how the Fourth,

---

[6] While *Beck* observed—in passing—that "circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an *increased* risk of future identity theft," 848 F.3d at 273 (emphasis added), it did not establish an actual disagreement on that question. No court has asserted that a *substantial* risk of identity theft is insufficient for standing.

Seventh, Eighth, and Ninth Circuits have all "reach[ed] analogous results" in data breach cases. *Lyshe v. Levy*, 854 F.3d 855, 860-61 (6th Cir. 2017). And in this case, the Ninth Circuit made clear that it used the same analysis as the Fourth, Seventh, Eighth, and D.C. Circuits did, and reached a "consistent" outcome. Pet. App. 12 n.6, 17 n.13.

B. Petitioner's manufactured circuit split does not exist.

Petitioner misinterprets the courts' applications of a single, fact-bound standard as legal disagreement among the courts of appeals. But there is none: No circuit has held that data breach victims can show injury-in-fact only when there is "misuse of the data," Pet. 11, and no circuit has held that "a breach itself [is] sufficient to confer Article III standing," *id.* 13.

1. Petitioner maintains that four circuits (the First, Second, Fourth, and Eighth Circuits) have adopted the rule that standing exists only when data breach victims' "information has actually been misused." *See* Pet. 1-2. But petitioner is mistaken: These four circuits apply the same fact-bound standard that all of the other circuits do.

a. Petitioner is incorrect that *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012), held "actual misuse" is a prerequisite to standing, Pet. 11, 15. *Katz* did not even involve a data breach. The plaintiff claimed only that defendant's data-*sharing* practices created a "risk that someone *might* access her data." *Katz*, 672 F.3d at 80 (emphasis added). The First Circuit held that the plaintiff did not allege a substantial risk of future harm because her allegations were "unanchored to any actual incident of data breach." *Id.*

In a case *Katz* cited that actually involved a data breach, *Anderson v. Hannaford Bros.*, 659 F.3d 151 (1st Cir. 2011), the First Circuit rejected the rule petitioner ascribes to it. There, the First Circuit held that victims alleged "cognizable injuries," even though they "d[id] not allege that they experienced any unauthorized charges." *Id.* at 165. As *Katz* explained, in *Anderson*, "confidential data actually ha[d] been accessed through a security breach." *Katz*, 672 F.3d at 80 (citing *Anderson*, 659 F.3d at 164-65). And the court in *Anderson* ultimately allowed the plaintiffs to recover the reasonable costs of identity theft insurance. *Anderson*, 659 F.3d at 165-67.

b. The Second Circuit has not issued any opinion with precedential effect on the question presented. In any event, *Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89 (2d Cir. 2017), held that the sole plaintiff in that case did not plausibly face a threat of future fraud "because her stolen credit card was promptly canceled after the breach and no other personally identifying information . . . [was] stolen." *Id.* at 90. That summary order says nothing about whether only already-defrauded plaintiffs can sue.

District courts in the Second Circuit interpret *Whalen* as consistent with decisions on the other side of petitioner's non-existent split. The Southern District of New York stated that *Whalen* "suggest[s] that [the Second Circuit] will follow the lead of its sister circuits"—the D.C., First, Sixth, and Seventh Circuits—which "consistently have held that Article III does not require Plaintiffs to wait for their identities to be stolen before seeking legal recourse." *Sackin*, 278 F. Supp. 3d at 746; *see also Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333, 340

(W.D.N.Y. 2018) (concluding that "*Whalen* strongly implies that the Second Circuit" would hold "that a risk of future identity theft is sufficient to plead an injury in fact"). In *Sackin*, the court accordingly held that the plaintiffs—whose identities had not yet been stolen—had standing because of the sensitivity of the stolen PII (including birthdates and social security numbers) and the nature of the theft (a company gave employees' PII directly to cybercriminals via a phishing email). 278 F. Supp. 3d at 746-47.

c. The Fourth Circuit's standing analysis reflects the same fact-bound substantial-risk standard, not a rule that requires actual misuse. In *Beck v. McDonald*, 848 F.3d 262 (4th Cir.), *cert. denied*, 137 S. Ct. 2307 (2017), the court held that a group of plaintiffs did not have standing after their healthcare provider lost some boxes and a laptop containing patient data. *Id.* at 266-68. The court explained that despite "extensive discovery," the plaintiffs did not show that "the thief stole the laptop with the intent to steal their private information," or even that their information had been "accessed." *Id.* at 274. This lack of evidence was dispositive at the summary judgment stage, where plaintiffs' allegations no longer enjoyed the presumption of truthfulness. *Id.* at 270 ("[T]he procedural posture of the case dictate[d] the plaintiff's burden . . . .").

To be sure, the court in *Beck* also noted that the plaintiffs did not allege their information was "accessed or misused or that they ha[d] suffered identity theft." 848 F.3d at 274. But that observation did not, as petitioner now maintains, announce any standing requirement. *See* Pet. 14-15. The observation

was simply one fact among many deficiencies showing the lack of any cognizable injury.[7]

Indeed, district courts understand that the Fourth Circuit requires an assessment of all of the facts to determine whether data breach victims have alleged an injury-in-fact. Courts have rejected the suggestion that "*Beck* precludes a finding of standing based on loss of personal information." *See, e.g.*, *Alston v. Freedom Plus/Cross River*, No. TDC-17-0033, 2018 WL 770384, at *4 (D. Md. Feb. 7, 2018).

d. The Eighth Circuit's injury-in-fact analysis likewise depends on a holistic assessment of the facts. In *In re SuperValu*, *Inc.*, 870 F.3d 763 (8th Cir. 2017), the court determined that a group of plaintiffs did not have standing based on the totality of the "facts pleaded by plaintiffs here," *id.* at 769—including how the theft was carried out (installed software), where the theft occurred (retail grocery stores), and the type of data stolen (credit card information), *id.* at 768-70.

Although the court observed that plaintiffs did not allege actual misuse, *SuperValu*, 870 F.3d at 769-70, its analysis did not stop there. Rather, the court explained that plaintiffs "relie[d] solely" on a 2007 government report as "factual support for the otherwise bare assertion" that data breaches

---

[7] Petitioner cites a later Fourth Circuit case for the unremarkable proposition that "mere compromise of personal information, without more," is insufficient for standing. Pet. 15 (quoting *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018)). But the court in *Hutton* did not require actual misuse or hold that only unreimbursed fraudulent charges qualify as misuse. Indeed, the court there recognized standing for data breach victims who had not incurred fraudulent charges. 892 F.3d at 617-19.

sometimes lead to identity theft. *Id.* at 770. While the report taken alone was insufficient to establish injury-in-fact, the court made clear that a plaintiff could "plausibly plead" a substantial risk of identity theft with "more detailed factual support." *Id.* at 770-71.

Petitioner is therefore incorrect that in the Eighth Circuit actual misuse is a prerequisite for standing. In *SuperValu*, the court explicitly declined to hold that "evidence of misuse following a data breach is necessary for a plaintiff to establish standing," calling that holding "a conclusion [the court] need not definitively reach today." 870 F.3d at 773.

2. The other five circuits petitioner discusses (the D.C., Third, Sixth, Seventh, and Ninth Circuits) rely on the same fact-bound substantial-risk standard. None of the five circuits has adopted the rule that petitioner attributes to all of them—that plaintiffs can establish standing "simply by alleging that a database . . . was breached." *See* Pet. 11.

a. In *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018), the D.C. Circuit held only that the plaintiffs plausibly alleged a substantial risk of identity theft. The plaintiffs' allegations supported the inference that hackers had "both the intent and the ability to use [the] data for ill," *id.* at 628, particularly because of the highly sensitive "nature of the data" that had been taken (which included social security, credit card, and health insurance numbers), *id.* at 629. Judge Griffith's opinion also stressed "the light burden of proof . . . at the pleading stage." *Id.* at 627.

Recent cases within the D.C. Circuit underscore that petitioner's interpretation of *Attias* is incorrect; the court did not hold "a breach itself sufficient to

confer Article III standing," Pet. 13. As the district court recently explained, "[n]either the Supreme Court nor the U.S. Court of Appeals for the D.C. Circuit has held that the fact that a person's data was taken is enough by itself to create standing to sue." *In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig.*, 266 F. Supp. 3d 1, 9, 20 (D.D.C. 2017) (reasoning that the court was "constrained to find that plaintiffs cannot predicate standing on the basis of the breach alone"). Rather, *Attias* was based "on a particular cybercrime in a commercial setting" and "did not purport to address every data breach." *Id.* at 35; *cf. In re Sci. Apps. Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 19 (D.D.C. 2014) ("[T]he mere loss of data . . . does not constitute [injury-in-fact].").

b. In the Third Circuit, the standing analysis also depends on the specific allegations before the court. In *In re Horizon Healthcare Services, Inc. Data Breach Litigation*, 846 F.3d 625 (3d Cir. 2017), the court held that a group of plaintiffs had standing under the Fair Credit Reporting Act to enforce their "*statutory* right to have their personal information secured against unauthorized disclosure." *Id.* at 634-35 (emphasis added). It did not, as petitioner maintains, conclude the plaintiffs had standing because they faced a substantial risk of future harm. *See* Pet 17-18. The court never reached that issue. *Horizon*, 846 F.3d at 639 & n.19.[8]

---

[8] The court merely observed that "[t]he facts of this case suggest that the data breach did create a 'material risk of harm,'" 846 F.3d at 639 n.19 (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016)), but not due to the breach alone. *Id.* (noting that the theft was "directed towards" acquiring "highly personal" information that "could be used to steal one's identity").

The Third Circuit's substantial-risk analysis in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), turned on the same case-specific factors that other courts apply. In *Reilly*, the plaintiffs lacked standing because it was "not known whether the hacker read, copied, or understood the data," *id.* at 40; "there [was] no evidence that the intrusion was intentional or malicious," *id.* at 44; and no plaintiffs had alleged any misuse, *id.* The court also distinguished cases from the Seventh and Ninth Circuits on the ground that the alleged harms in those cases were "significantly more 'imminent'" than the alleged harms in *Reilly*. *Id.*

c. The Sixth Circuit also performs a holistic assessment of the facts surrounding each data breach. In *Galaria v. Nationwide Mutual Insurance Co.*, 663 Fed. Appx. 384 (6th Cir. 2016), the court recognized standing because hackers deliberately "target[ed]" highly sensitive PII (including social security numbers, driver's license numbers, and birthdates). *Id.* at 386, 388-89. The court also highlighted that plaintiffs had proposed to supplement their complaint with evidence of unauthorized attempts to open credit cards in their names. *Id.* at 389 n.1. It did not conclude there was standing "simply by virtue of the breach." *See* Pet. i.

d. The Seventh Circuit's analysis works the same way. The court in *Remijas v. Neiman Marcus Group*, 794 F.3d 688 (7th Cir. 2015), concluded that a group of plaintiffs had standing based on how the theft was executed—through a sophisticated string of cyberattacks that targeted a database containing payment card numbers, social security numbers, and birthdates. *Id.* at 690. Hackers used malware to obtain

card information and plaintiffs incurred several fraudulent charges. *Id.*

Contrary to petitioner's claim, the Seventh Circuit has never conferred standing "regardless of whether [plaintiffs] allege any actual identity theft or fraud." *See* Pet. 17. All of the Seventh Circuit cases that petitioner cites included allegations of prior fraud. *See Remijas*, 794 F.3d at 693-94 (noting that "9,200 [credit] cards ha[d] experienced fraudulent charges"); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965 (7th Cir. 2016) (recounting how data breach victims alleged "four fraudulent transactions"); *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 827 (7th Cir. 2018) (observing that customers suffered "unauthorized charges" to bank accounts).

Nor do district courts believe that the Seventh Circuit recognizes standing whenever there is a data breach. In fact, they have denied standing in cases where plaintiffs' information was compromised in a data breach. *See, e.g.*, *In re VTech Data Breach Litig.*, No. 1:15-cv-10889, 2017 WL 2880102, at *4 (N.D. Ill. July 5, 2017).

e. The law in the Ninth Circuit is just like the law everywhere else—a holistic, fact-bound standard. In this case, for example, the court held only that the "sum of [plaintiffs'] allegations" established (at the pleading stage) a "substantial risk" of fraud or identity theft. Pet. App. 16-17. Underscoring the fact-specific nature of the legal standard, the Ninth Circuit has denied standing in cases where defendants negligently disclosed plaintiffs' PII. In *Bassett v. ABM Parking Services, Inc.*, 883 F.3d 776 (9th Cir. 2018), the court held that plaintiffs did not face a substantial risk of future harm after defendants illegally exposed the

plaintiffs' credit card expiration dates. *Id.* at 777; *see also Daniel v. Nat'l Park Serv.*, 891 F.3d 762, 765 (9th Cir. 2018) (same).

District courts in the Ninth Circuit understand that its standing analysis reflects a fact-bound standard, not a rule that a "breach itself [is] sufficient" for "Article III standing." *See* Pet 13. Courts have relied on the Ninth Circuit's opinion in this case to deny standing when a particular data breach does not put plaintiffs at a substantial risk of future harm. In *Antman v. Uber Technologies, Inc.*, No. 15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018), a district court denied standing to a group of Uber drivers whose driver's license and banking numbers were downloaded by hackers. *Id.* at *1, *11; *see also Brett v. Brooks Bros. Grp., Inc.*, No. CV 17-4309-DMG (Ex), at 4-7 (C.D. Cal. Sept. 6, 2018) (citing the opinion in this case and denying standing); *cf. Dugas*, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016) (denying standing because the theft of customer data was "far more limited" and included less "useful personal information" than in other cases).

II. This case does not raise a substantial question of nationwide importance.

A. Deciding this case will not resolve standing in all "data breach" cases.

Determining whether the plaintiffs in *this* case alleged, much less established, an injury-in-fact would not help lower courts resolve whether other data breach victims have established an injury-in-fact for at least two reasons. First, because the factual variation among data breaches necessarily shapes courts' substantial-risk analyses, reviewing this case would

provide limited guidance to other courts grappling with other kinds of data breaches. Second, the existence of statutorily defined injuries-in-fact—present in many data breach cases but not this one—elevates some injuries to cognizable harms.

1. The fact-bound nature of the substantial-risk standard limits the guidance this Court could provide to lower courts by reviewing the court of appeals' application of the substantial-risk standard to this particular breach. Substantial-risk analyses necessarily turn on myriad variations among data breaches, including what kind of data was compromised, how it was compromised, and how it might be misused.

a. Reviewing the Ninth Circuit's decision here would provide little guidance in cases involving different kinds of compromised data.

The risk of harm to data breach victims depends on the "nature of the data" compromised in a breach. *Attias*, 865 F.3d at 629. The exposure of only names and addresses, for example, poses less risk than the release of credit card numbers, email addresses, and passwords together. Fraudsters can make less use of credit card numbers alone than credit card numbers linked to names, addresses, CVVs, and PINs. *Compare Donna Karan*, 872 F.3d at 115 (first six and last four digits of credit card number), *and Whalen*, 689 Fed. Appx. at 90 (payment card number), *with Dieffenbach*, 887 F.3d at 827 (card number, name, address, and PIN). Compromised medical data and social security numbers raise different risks, too. *Attias*, 865 F.3d at 629.

Data-storage methods also engender different risks. Encrypted data poses less risk than unencrypted

data. *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010). And encryption methods that can be circumvented with a compromised key create more risk than more sophisticated protections. *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1206-07 (N.D. Cal. 2014).

b. Courts confronting different ways that data is compromised would gain little from reassessing the risks of the precise "factual scenario this case presents"—a hacked database. *See* Pet. 30.

Different methods of exposure present different risks. It is more likely that fraudsters will misuse data that was specifically targeted in a cyberattack than data incidentally acquired through physical theft. *Compare Beck*, 848 F.3d at 267-68 (lost or stolen laptop and storage boxes), *with Galaria* 663 Fed. Appx. at 386 (cyberattack). Victims face more risk when hackers deliberately take data than when data-holders accidentally expose it. *Compare Remijas*, 794 F.3d at 688 ("[H]ackers deliberately targeted . . . credit-card information."), *with Bassett*, 883 F.3d at 777 (data-holder negligently printed excessive credit card information on receipts). And phishing schemes pose their own risks. *See Sackin*, 278 F. Supp. 3d at 746, 748 ("PII here was provided directly to cybercriminals [through a phishing scheme], and not merely printed on a store receipt.").

Different entities may also be targeted for different reasons, as data breaches occur across sectors, including "business, banking/credit/financial, educational, Government/Military[,] and medical/healthcare." Identity Theft Res. Ctr., *supra*, at 19; *see also U.S. Office of Pers. Mgmt.*, 266 F. Supp. 3d at 8 (government agency); *Beck*, 848 F.3d at 266

(veterans medical center); *Galaria*, 663 Fed. Appx. at 385 (insurance company); *SuperValu*, 870 F.3d at 765 (grocery store); Pet. App. 26 (online retailer owned by Amazon).

And while data is occasionally stolen, sometimes it is merely accessed. In some cases, hackers "harvest[] the data on the network," *SuperValu*, 870 F.3d at 766; in others, hackers may not have "read, copied, or understood the data," *Reilly*, 664 F.3d at 40.

c. Reviewing this case will not help lower courts address breaches that raise risks of different *forms of misuse* than are at issue here.

Substantial-risk analyses turn on *how* plaintiffs' information could be misused. This case involves the risk of fraudulent use of email, credit card, and online retail accounts; fraudulent creation of new accounts; and phishing and pharming. Compl. ¶¶ 34, 40, 43, 48, 67, 71-72. But those are hardly the only kinds of misuse that might arise from data breaches. *See, e.g.*, *Attias*, 865 F.3d at 628 ("medical identity theft"); *Horizon*, 846 F.3d at 630 ("fraudulent tax return"); *Remijas*, 794 F.3d at 691 ("a scam through her cell phone"). And different kinds of misuse materialize on different timelines. *See Attias*, 865 F.3d at 628 (noting that victims may not learn about medical identity theft until their insurance is depleted).

d. Reviewing this case will not provide meaningful guidance to lower courts as technology develops in ways that alter risks to data breach victims.

Cybercriminal activity is a "threat landscape that constantly evolves." Dep't of Justice, *Report of the Attorney General's Cyber Digital Taskforce* 23 (2018), https://bit.ly/2uBnIbX. Hackers can steal data with

new tools like artificial intelligence, changing the danger posed by cybersecurity threats. *See* Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* 4-6 (2018), https://bit.ly/2EV6NHL. New technologies may also change the ways data is stored and protected. *Id.*

Further, the type and amount of vulnerable PII continues to change. For instance, smart phone data, including geolocation information, creates an alarmingly comprehensive personal profile. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018). And biometric databases contain an increasing amount of highly personal data, including retinal scans, fingerprints, and genetic profiles. *See, e.g.*, Huizhong Wu, *Alleged Breach of India's Biometric Database Could Put 1.2bn Users at Risk*, CNN (Jan. 11, 2018), https://cnn.it/2RuSfkO; *Frequently Asked Questions on CODIS and NDIS*, FBI.gov, https://bit.ly/2jLVUup (last visited Nov. 5, 2018). As types of data and breaches evolve, along with the ways data is stored, this Court would "face the embarrassment of explaining in case after case that the principles on which [its] decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered." *Carpenter*, 138 S. Ct. at 2261 (Alito, J., dissenting).

2. Reviewing this case also would not resolve whether other data breach victims have established an injury-in-fact. Many courts' standing determinations depend on a factor not present here: statutorily defined injuries-in-fact.

Statutorily defined injuries-in-fact significantly affect whether plaintiffs have standing. Congress may

"elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 578 (1992)). In the Third Circuit, congressionally defined injuries may "elevate disclosure[s] of private information into a concrete injury." *Horizon*, 846 F.3d at 640-41 n.23. The court in *Horizon* bypassed a substantial-risk analysis because "improper disclosure of one's personal data in violation of [the] FCRA" alone sufficed as a "cognizable injury for Article III." *Id.* at 641. The Eighth Circuit has likewise suggested that a statutory injury, together with allegations of a "material risk of harm"—rather than a substantial risk of harm—might confer standing. *Braitberg v. Charter Comms., Inc.*, 836 F.3d 925, 930 (8th Cir. 2016); *see also Brown v. R & B Corp. of Va.*, 267 F. Supp. 3d 691, 697 (E.D. Va. 2017) ("[A] procedural violation that presents a 'risk of real harm' to a substantive right" may independently suffice for standing.).

Data-breach plaintiffs frequently bring federal statutory claims. In several of the post-*Spokeo* cases petitioner cites, plaintiffs alleged violations of federal privacy or consumer-protection statutes.[9] Since this case does *not* implicate federal statutory injuries, its reconsideration would provide no guidance to lower courts in cases involving such claims.[10]

---

[9] *See Horizon*, 846 F.3d at 629; *Beck*, 848 F.3d at 266; *Galaria*, 663 Fed. Appx. at 385.

[10] The district court previously dismissed respondents' FCRA claim for failure to state a claim. Order 5-6, Sept. 9, 2013, ECF No. 114.

B. This case does not have the dire economic implications petitioner suggests.

1. Continuing to apply this Court's established Article III standing jurisprudence in data breach cases will not result in blameless defendants being held liable for every data breach. *See* Pet. 28-31.

Persons and entities with reasonable and appropriate security measures have nothing to fear. Established legal tools such as motions to dismiss for failure to state a claim protect defendants from unwarranted legal liability.[11] So do motions for summary judgment. *See, e.g.*, *Beck*, 848 F.3d at 270. And, in any event, defendants that "design their systems properly," Pet. 1, will prevail on the merits.

2. Contrary to what petitioner argues, the decision below does not "severely dull[] incentives to take immediate steps to prevent actual misuse of the data" after a breach. Pet. 3; *see id.* 12.

Petitioner wrongly presumes that avoiding lawsuits is the only reason why data-holders make any effort to meaningfully respond to data breaches once they occur. U.S.-based data-holders have a strong incentive to respond to data breaches to avoid losing business. Ponemon Inst., *2018 Cost of a Data Breach Study: Global Overview* 29 (2018), https://bit.ly/2M7zZPB. The industry experts

---

[11] Cases dismissed on this ground include cases identified by petitioner's amici. *See* Br. of Chamber of Commerce in Support of Petitioner at 18 (citing *Cahen v. Toyota Motor Corp.*, No. 3:15-cv-01104 (N.D. Cal. Mar. 10, 2015); *In re VTech Data Breach Litig.*, No. 1:15-cv-10889 (N.D. Ill. Apr. 18, 2018)); *see also In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2018 WL 1189327 (D. Minn. Mar. 7, 2018).

petitioner identifies concluded that data-holders' incident response teams are the most effective way to minimize costs after a data breach. *See id.* at 22 fig.12; Pet. 29 (citing the same report). Further, the specter of liability naturally incentivizes companies to adopt better data-security measures.

III. This case does not cleanly present petitioner's legal question.

A. Petitioner's legal contentions are interlaced throughout with impermissible factual disputes.

The operative facts for the standing analysis here are the factual allegations in respondents' complaint. This case arises from a motion to dismiss, at which point courts are required to accept as true all plausible allegations in the complaint. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007).

1. Petitioner bases its standing argument on the representation that its customers' passwords were stored in a "cryptographically scrambled state,"[12] and that only "[p]artial credit card information may . . . have been accessed." Pet. 4-5. But respondents plausibly allege that Zappos.com "fail[ed] to properly encrypt the[ir] PII" and that full payment card information was compromised. Compl. ¶¶ 62, 64, 66-67.

These facts matter to the standing analysis. Accepting petitioner's version of the facts presents a different case than this one. And because this Court

---

[12] For this proposition, petitioner cites to pages in its appendix, Pet. App. 47-48, 65-66, that do not identify any cryptographic scrambling of passwords in this case.

cannot review those facts at this stage in litigation, it cannot reach petitioner's question.

2. Accepting respondents' version of the facts does not leave petitioner without a way to challenge them. Petitioner may challenge the allegations in the complaint in a motion for summary judgment. Both sides would then have the benefit of full discovery—now stayed—to substantiate whatever legal arguments they may wish to make.[13]

B. This case involves allegations of misuse.

Named plaintiffs and similarly situated parties—victims of the same breach—alleged misuse. This case therefore does not implicate the question petitioner has raised: whether plaintiffs who did not allege that their data has been "put to misuse" can nevertheless demonstrate injury-in-fact. *See* Pet. 21.

1. Petitioner is wrong to argue that "plaintiffs concededly have suffered no misuse of their own data." Pet. 2. To the contrary, respondents plausibly pleaded that fraudsters hijacked Hasner and Nobles's email accounts. Compl. ¶¶ 34, 40.

Petitioner does not explain why the harm Hasner and Nobles experienced is not "misuse." Nor does it offer a consistent account of what constitutes misuse. *Compare* Pet. 2 (acknowledging that "two dozen" Zappos.com customers "claimed that their data were misused"), *with id.* 22 n.2 (suggesting that it is unclear whether it would be "sufficient for Article III standing"

---

[13] The court below recognized that, "beyond the pleadings stage," the complaint's allegations alone "will not sustain [p]laintiffs' standing" without additional evidence. Pet. App. 16 n.12 (citing *Lujan*, 504 U.S. at 561).

if respondents "*had* suffered some credit irregularities or fraudulent charges" but were not "forced to foot the bill"). It is thus uncertain how the rule that petitioner asks this Court to adopt would apply to the facts of this case, much less any other.

2. Petitioner further complicates this case by arguing that courts may consider only those allegations of misuse involving respondents' own PII. *See* Pet. 26 (asserting that respondents may not "bootstrap their way into Article III by pointing to *other* individuals' purported injuries"). But the misuse of similarly situated victims' PII is relevant to assessing whether respondents face a substantial risk of harm. And petitioner cites no authority in support of its incorrect view that this Court should ignore well-pleaded facts in the complaint.

Here, beyond the harm to named plaintiffs, respondents also alleged that other victims of the same breach suffered misuse. Twenty-seven customer complaints evidenced widespread PII misuse, and at least half identified successful theft and fraud. Compl. ¶ 67. The allegations about O'Brien and Wadsworth—who were named plaintiffs in the district court—identified additional instances of misuse. Respondents' complaint alleged that O'Brien and Wadsworth incurred fraudulent charges and out-of-pocket financial losses, among other harms. Compl. ¶¶ 43-44, 48.

Under this Court's precedent, these allegations may substantiate respondents' claims of concrete injury. In *Susan B. Anthony List*, this Court considered past instances of similar harm suffered by others to evaluate the likelihood of future harm to plaintiffs. 134 S. Ct. at 2345-46; *see also Steffel v.*

Thompson, 415 U.S. 452, 459 (1974) (reasoning that a previous prosecution of another individual can provide "ample demonstration" that a plaintiff's alleged future harm is not "chimerical" (quoting *Poe v. Ullman*, 367 U.S. 497, 508 (1961))).

Lower courts do the same in data breach cases. Fraudulent charges incurred by a non-plaintiff victim of the same data breach can "inform[] [a court's] analysis of whether the risk of identity theft facing . . . [p]laintiffs is substantial and well-founded." *Moyer v. Michaels Stores, Inc.*, No. 1:14-cv-00561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014) (citing *Susan B. Anthony List*, 134 S. Ct. at 2345-46).

Because this case involves allegations of misuse, it does not cleanly present the legal issue that petitioner manufactured.

IV. The court of appeals decision is correct.

A. Respondents plausibly alleged an injury-in-fact.

The Ninth Circuit correctly determined that respondents "sufficiently alleged an injury in fact based on a substantial risk that the Zappos hackers will commit identity fraud or identity theft." Pet. App. 16-17.

1. The Ninth Circuit properly credited the allegations in respondents' complaint. The sensitive nature of the stolen data supported the conclusion that it could "be used to commit identity theft." Pet. App. 13. So did the allegations that Hasner and Nobles's email accounts were commandeered, that O'Brien and Wadsworth incurred fraudulent charges, and that twenty-seven victims experienced various forms of unauthorized account activity. *Id.* 13 n.7, 14.

The passage of several years since the breach did not make the risk of harm less concrete. Respondents pleaded that victims "may not see the full extent of identity theft or identity fraud for years." Pet. App. 16 (quoting Compl. ¶ 77). To support that allegation, respondents referenced a government report that revealed that "stolen data may be held" for some time[14] before criminals trade it on the "cyber black-market" indefinitely. Compl. ¶ 80.

The Ninth Circuit recognized that petitioner's fixation on the passage of time failed to account for the way that data thieves use PII in the digital age. *See* Pet. App. 13. Cybercriminals use PII to lure victims into divulging more information, *id.*, and then assemble a full profile of a person's identity as if they were putting together a puzzle. Compl. ¶¶ 53-56. This "mosaic effect" takes years to unfold, as computer programs scan thousands of large public data sets; stolen password information from one website provides access to others;[15] and the different data elements "link" various pieces of information to an individual. *See id.*

2. The Ninth Circuit squared its conclusion with this Court's decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), despite petitioner's claim that reconciling them is "impossible." Pet. 23. Petitioner correctly notes that

---

[14] Compl. ¶ 77 (quoting U.S. Gov't Accountability Office, GAO-07-737, *Personal Information* 29 (2007), https://bit.ly/2Oe7YTh).

[15] This is commonplace. *See* Pew Research Ctr., *Americans and Cybersecurity* (2017) (recognizing that thirty-nine percent of people use the same or similar passwords on multiple websites).

"*Clapper* could not have been clearer that an actual injury must be *imminent*, not just possible, to give rise to Article III standing." *Id.* 18. The Ninth Circuit concluded that harm to respondents *is* "imminent." Pet. App. 15. It explained that unlike in *Clapper*, where the harm to plaintiffs depended on an attenuated series of contingent events (none of which had yet occurred), hackers here have already targeted, accessed, and misused respondents' PII. *See id.* 10-11, 14. At any rate, the standing analysis in *Clapper* was "especially rigorous" because the plaintiffs had challenged government action related to national security. Pet. App. 11 (quoting *Clapper*, 568 U.S. at 408). That is not true here.

B. Petitioner's arguments go to the merits of the case, not standing.

Petitioner's insistence that it was the "direct victim" of an unpreventable hack, Pet. 27, is irrelevant to whether respondents have alleged an injury-in-fact. Petitioner's argument "confus[es] . . . the merits with . . . Article III standing," despite this Court's repeated warnings not to conflate the two. *Ariz. State Legislature v. Ariz. Indep. Redistricting Comm'n*, 135 S. Ct. 2652, 2663 (2015) (quoting *Davis v. United States*, 564 U.S. 229, 249 n.10 (2011)).

If petitioner is correct that respondents lack standing because "specific allegations of resulting misuse" are required to demonstrate injury-in-fact, Pet. 11, then plaintiffs would also lack standing to sue a company that *willfully* sold their personal information to cybercriminals, at least until they incurred fraudulent charges. If petitioner is wrong, and data breach victims have standing if a company willfully sells their personal information on the black

market, then petitioner's liability-focused arguments do not establish a lack of injury-in-fact. Rather, they go to the merits of the case.

C. Petitioner's proposed rule for injury-in-fact makes no sense.

1. Petitioner's injury-in-fact arguments are inconsistent with this Court's precedent. This Court has repeatedly recognized that a substantial risk of future harm gives rise to standing. *Clapper*, 568 U.S. at 409. In *Susan B. Anthony List*, this Court reiterated that principle and held that plaintiffs had standing because they anticipated engaging in statutorily proscribed political speech, even though the plaintiffs themselves had not been previously harmed. 134 S. Ct. at 2345.

Despite these cases, petitioner suggests that "specific allegations of resulting misuse" are required to establish injury-in-fact, Pet. 11, and that data breach victims do not face a "substantial risk" of harm until their data is actually "put to misuse by the perpetrator of the attack," Pet. 21. That argument confuses the past with the future, and it contradicts this Court's recognition that future harm is a separate category of injury-in-fact.

2. Eliminating the risk of future harm as a category of injury-in-fact would harm data breach victims. It would do away with remedies, such as credit monitoring or other forms of prospective relief, that could prevent victims' information from actually being misused. Victims often pursue these remedies because of their value in protecting compromised PII. *See* Pet. App. 19; *see also Horizon*, 846 F.3d at 632; *Hutton*, 892

F.3d at 617; *Beck*, 848 F.3d at 267; *Galaria*, 663 Fed. Appx. at 387; *Remijas*, 794 F.3d at 690.

Petitioner's proposed rule would also mean that victims may not be able to recover damages even for injuries that have already occurred, but are not discovered until after the applicable statute of limitations has run. State common law and statutory provisions impose narrow time limits during which it may be difficult, if not impossible, to uncover evidence of fraud. The California consumer protection statutes at issue in this case, for example, along with the state's causes of action for fraud and unjust enrichment, have statutes of limitations of just three years. Cal. Civ. Code § 1783; Cal. Code Civ. P. § 338(c)(1), (d).

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be denied.

Respectfully submitted,

Gregory D. Blankinship
Jeremiah Frei-Pearson
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
445 Hamilton Ave.
Suite 605
White Plains, NY 10601

Marc L. Godino
GLANCY, PRONGAY & MURRAY, LLP
1925 Century Park East
Suite 2100
Los Angeles, CA 90067

Ben Barnow
Counsel of Record
Erich P. Schork
BARNOW & ASSOCIATES, P.C.
1 N. LaSalle St., Suite 4600
Chicago, IL 60602
(312) 621-2000
b.barnow@barnowlaw.com

Richard L. Coffman
THE COFFMAN LAW FIRM
505 Orleans St., Fifth Floor
Beaumont, TX 77701

David C. O'Mara
THE O'MARA LAW FIRM, P.C.
311 E. Liberty St.
Reno, NV 89501

November 6, 2018