No. 18-225

In the Supreme Court of the United States

ZAPPOS.COM, INC.,

Petitioner,

v.

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

Respondents.

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

BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AND NATIONAL RETAIL FEDERATION AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

STEVEN P. LEHOTSKY
U.S. Chamber Litigation Center
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

STEPHANIE MARTZ
National Retail Federation
1101 New York Ave, NW
Washington, DC 20005
(202) 783-7971

ANDREW J. PINCUS
Counsel of Record
RAJESH DE
STEPHEN C.N. LILLEY
MATTHEW A. WARING
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES—continued

Page(s)

RULES

TABLE OF AUTHORITIES—continued

Page(s)

MISCELLANEOUS

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AND NATIONAL RETAIL FEDERATION AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

INTEREST OF THE *AMICI CURIAE*

The Chamber of Commerce of the United States of America is the world's largest business federation. It represents 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country.[1]

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

Amicus the National Retail Federation ("NRF") is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants, and internet retail-

[1] Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici*, their members, and their counsel made a monetary contribution to its preparation or submission. Counsel of record for all parties received notice at least 10 days prior to the due date of the intention of *amici* to file this brief. All parties consented to the filing of the brief.

ers from the United States and more than 45 countries. Retail is the largest private-sector employer in the United States, supporting one in four U.S. jobs—approximately 42 million American workers—and contributing $2.6 trillion to annual GDP. In accordance with applicable legal limitations, NRF's members gather data from their customers through both in-store and online transactions. As the industry umbrella group, NRF periodically submits *amicus curiae* briefs in cases raising significant legal issues, including the specific issue of the standing that is required to enforce data privacy and security laws, which are important to the retail industry at large, and particularly to NRF's members. A recent example is *Rosenbach* v. *Six Flags Entertainment Corp.*, No. 123186 (Ill. Sup. Ct.).

Amici have a significant interest in the Article III standing issue presented by this case because their members frequently face putative class action lawsuits alleging claims arising from data breaches, without allegations that the plaintiff has suffered any injury beyond a speculative risk of harm in the future. This Court held in *Clapper* v. *Amnesty International USA*, 568 U.S. 398, 416 (2013), that a "risk of harm" in the future suffices to confer standing only if the future harm is "certainly impending" rather than merely possible.

If, despite the mandate of *Clapper*, plaintiffs are permitted to pursue cases like this one, *amici*'s members will be mired in lawsuits over data breaches that have not caused any actual or imminent harm to the plaintiffs—but which threaten to extract massive settlements from businesses that were victimized by hackers or thieves. *Amici* therefore urge the Court to grant review in this case to ensure faith-

ful adherence to Article III's standing requirements, which enable the federal courts to be available to lawsuits addressing real harms but closed to lawsuits that are designed to force costly settlements rather than redress concrete harms.

INTRODUCTION AND SUMMARY OF ARGUMENT

Five courts of appeals—including the court below—have held (in conflict with four other courts of appeals) that a plaintiff can satisfy Article III's standing requirement simply by alleging that his or her personal information was involved in a data breach. As a result, plaintiffs' lawyers in these five circuits can and do routinely bring suit soon after a business announces that it has suffered a data breach—even though there is no evidence that consumers have suffered actual harm, or any indication that such harm is imminent. The question whether this extraordinarily generous approach to standing in data breach cases is correct is manifestly worthy of this Court's review, for two reasons.

First, this approach cannot be squared with this Court's precedents—most prominently, *Clapper* v. *Amnesty International USA*, 568 U.S. 398 (2013)—holding that a risk of harm in the future does not satisfy Article III's injury-in-fact requirement unless the threatened harm is "certainly impending." When all that is known is that a company has experienced a data breach, a court cannot conclude that consumers face a "certainly impending" risk of identity theft, and consequent harm, without speculating about whether and when consumers' personal information might be misused. *Clapper* makes clear that such speculative reasoning, built on chains of inferences

about the possible choices of third parties, cannot support standing.

Second, the impermissibly overbroad approach to standing reflected in the decision below incentivizes plaintiffs' lawyers to rush to the courthouse as soon as a data breach is disclosed—before many facts are gathered and before much is known about the breach's likely consequences—in search of a quick settlement payout. This abusive form of litigation—producing litigation costs and settlement payments divorced from the underlying merits of the claim—imposes very significant costs on the business community and serves no useful purpose. This Court should overturn the standing holding below, which is a critical enabler of these unjustified practices.

ARGUMENT

I. The Decision Below Is Irreconcilable With *Clapper*.

Although the Ninth Circuit purported to apply this Court's decision in *Clapper*, that court—like the other courts on its side of the circuit conflict—adopted, in effect, a categorical rule that the theft of personal information in a data breach *automatically* creates a risk of future harm that satisfies Article III. This *per se* approach to standing in data breach cases squarely conflicts with *Clapper*.

A. *Clapper* Requires "Certainly Impending" Future Harm or a "Substantial Risk" of Such Harm.

In *Clapper*, this Court reiterated its "well-established requirement that threatened injury must be 'certainly impending'" to establish Article III standing. 568 U.S. at 401 (quoting *Whitmore* v. *Ar-*

kansas, 495 U.S. 149, 158 (1990)); *see also Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 564 n.2 (1992). Under that requirement, "'[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 568 U.S. at 409 (quoting *Whitmore*, 495 U.S. at 158).

The Court rejected the more lenient standard endorsed by the court of appeals in that case, which would have required only an "objectively reasonable likelihood" of future harm. *Id.* at 408. The Court further held that allegations of future harm cannot "rest on speculation about the decisions of independent actors" not before the Court or on a "speculative chain of possibilities." *Id.* at 414.

To be sure, *Clapper* recognized that plaintiffs in prior cases had not been required to plead that it was "literally certain that the harms they identify will come about." 568 U.S. at 414 n.5. But those decisions found standing, the Court emphasized, because there was a "substantial risk" of harm sufficiently certain to make "reasonabl[e]" the expenditure of "costs to mitigate or avoid that harm." *Ibid.* The Court expressed doubt that the "substantial risk" standard differed from the "clearly impending" test. *Ibid.* And it held that an "attenuated chain of inferences necessary to find harm" cannot satisfy either test—"to the extent the 'substantial risk' standard is * * * distinct from the 'clearly impending' requirement" at all. *Ibid.*; see also *Susan B. Anthony List* v. *Driehaus*, 134 S. Ct. 2334, 2341 (2014) ("An allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.") (citing *Clapper*, 568 U.S. at 414 n.5) (internal quotation marks omitted).

Clapper further held that plaintiffs "cannot manufacture standing merely by inflicting harm on

themselves based on their fears of hypothetical future harm that is not certainly impending." 568 U.S. at 416. To hold otherwise would "improperly water[] down the fundamental requirements of Article III" and allow "an enterprising plaintiff * * * to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Ibid.*

While *Clapper* involved a challenge to alleged government surveillance, the Court's articulation of Article III's requirements was not limited to that particular factual context. Indeed, this Court made that clear in *Spokeo, Inc.* v. *Robins*, a consumer class action, by pointing to *Clapper* to explain that a "risk of real harm" in the future may "satisfy the requirement of concreteness." *Spokeo*, 136 S. Ct. at 1549 (citing *Clapper*, 133 S. Ct. 1138); *see also id.* at 1550 (explaining that plaintiffs must allege a "material risk of harm"—*i.e.,* "a degree of risk sufficient to meet the concreteness requirement"). Thus, as the Fourth Circuit recognized, the inquiry into standing in the data breach context must be undertaken "with *Clapper*'s tenets firmly in tow." *Beck* v. *McDonald*, 848 F.3d 262, 273 (4th Cir. 2017).

B. The Occurrence Of A Data Breach—Standing Alone—Is Not Sufficient To Satisfy Article III.

The foregoing analysis makes clear that the fact that an individual's personal information is implicated in a data breach is not sufficient by itself to support Article III standing.

1. The court below held that respondents satisfied Article III by alleging "a substantial risk that the Zappos hackers will commit identity fraud or

identity theft." Pet. App. 16-17. But a "risk" based only on the occurrence of the data breach falls far short of what *Clapper* requires.

Respondents did not allege that the hackers were *likely* to use their personal information for nefarious purposes; they simply alleged that the information gave the hackers "the *means* to commit fraud or identity theft." Pet. App. 14 (emphasis added). The court of appeals therefore based its standing holding on the mere possibility that hackers *might* use the information obtained to commit identity theft in the future. That conclusion is wrong, for three reasons.

First, it is squarely foreclosed by *Clapper*, which "decline[d] to abandon" this Court's "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors." 568 U.S. at 414. That principle applies fully here: respondents' standing claim depends on the choices of unknown hackers who may or may not decide, or even be able, to inflict harm by misusing the information they obtained. The injury that respondents assert here is therefore only theoretically *possible*, rather than "certainly impending." *Id.* at 410.[2]

---

[2] Some courts of appeals have reasoned that a substantial risk of identity theft can be inferred from a hack of personal information, because the likeliest explanation for hackers' decision to attack a company is that they planned to engage in identity theft. See, *e.g.*, *Attias* v. *Carefirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017) (finding it "plausible * * * to infer that [the hacker] has both the intent and the ability to use [plaintiffs'] data for ill"); *Remijas* v. *Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers breach into a store's data base and steal consumers' private information"?). But that reasoning, too, relies entirely on speculation about the subjective intentions of unknown third parties that *Clapper* pre-

Second, the speculative nature of plaintiffs' fear of future identity theft is made all the more apparent by the staleness of the breach and lack of evidence of harm. The breach took place in January 2012—more than *six years* ago. And "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275 (internal quotation marks omitted).

The court of appeals ignored the amount of time that had passed without any incident involving respondents' information, because (1) it was a fact outside the complaint, and (2) the "relevant moment" for determining standing was the moment when the complaint was filed. Pet. App. 15-16 & n.12. But the lower court adopted a legal rule that the odds of harm from a data breach are so high that "certainly impending" injury can be presumed from the fact of the breach. The facts of this case surely are relevant to the permissibility of that conclusion. Indeed, the fact that respondents here have yet to suffer any actual harm is not unusual—it is commonplace for a risk of identity theft not to materialize for years after a breach, as the court of appeals itself acknowledged (Pet. App. 16 & n.12), and breaches often do not lead to any injury at all. See, *e.g.*, *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (discussing a Government Accountability Office report that had "concluded based on the available data and information that most breaches have not resulted in detected incidents of identity theft") (internal quotation marks

---

cludes. The standing inquiry must turn on the *actual* risk plaintiffs face as a result of the particular breach at issue, not generalized speculative assumptions about nonparties' behavior.

omitted. The risk facing respondents thus simply cannot be described as "certainly impending."

Finally, by basing standing solely on the fact that respondents' information was stored in a breached database, the court of appeals papered over critical factual details that are highly relevant in determining the likelihood that respondents will be harmed in the future. For instance, the court of appeals disregarded petitioner's representations that only the last four digits of customers' credit card numbers, not the entire numbers, were implicated in the breach. Pet. App. 5.

Plaintiffs in data breach cases should not be able to evade the significance of such facts. Put simply, not every attacker is seeking to commit identity theft. *See, e.g.*, Dep't of Justice, *Report of the Attorney General's Cyber Digital Task Force* 23 (July 2, 2018), https://justice.gov/cyberreport ("Various actors, with varying motivations, perpetrate these schemes, targeting various categories of victims.").

In short, the mere fact that a company has experienced a data breach involving personal information does not automatically establish the Article III standing of every single consumer whose information was affected by the breach. To find that every consumer faces a "certainly impending" risk of harm from the mere fact of a breach requires a series of speculative inferences about what information third parties obtained and what those third parties *might* do with the information—the exact inferential reasoning that *Clapper* forbids.[3]

---

[3] Indeed, the decision below went one step further, by finding that respondents had shown standing (in part) by alleging that

2. Some courts of appeals have also based findings of standing on expenditures by plaintiffs based on anxiety about identity theft—for example, on credit monitoring services or "mitigation costs." See, *e.g.*, *Galaria* v. *Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016); *Remijas*, 794 F.3d at 694. But these costs cannot support standing, for the same reasons that the *Clapper* plaintiffs' expenditures based on "subjective fear of surveillance" were found too speculative to satisfy Article III. 568 U.S. at 418. The *Clapper* Court squarely rejected the theory that plaintiffs can "establish standing by asserting that they suffer present costs and burdens that are based on a fear of [future injury], so long as that fear is not 'fanciful, paranoid, or otherwise unreasonable.'" *Id.* at 416 (citation omitted). That theory failed, the Court explained, "because the harm [that the plaintiffs] seek to avoid is not certainly impending." *Id.* To hold otherwise would "improperly water[]

---

they were at risk of "phishing" and "pharming," both of which are hacking techniques in which a threat actor obtains the victim's information by inducing the victim to open a legitimate-looking email or website and click on a link or otherwise provide their sensitive information. But finding standing on this basis requires not only inferring that a third party will target respondents with a phishing or pharming attack in the future but that the targeted consumers will be fooled by the attack and disclose sensitive information or click on a malicious link, leading to the successful installation of malware that functions as intended, and also assuming that the hacker will use relevant information harvested by the malware during the time that information remains valid. If it is improper for a court to speculate about the future actions of third parties (see *Clapper*, 568 U.S. at 414), it is just as improper for a court to speculate about what plaintiffs themselves may do *in response* to the actions of third parties.

down the fundamental requirements of Article III." *Ibid.*

In other words, allegations of expenditures based on risk of future harm cannot override *Clapper*'s "certainly impending" inquiry. Without future harm that is "certainly impending," self-inflicted mitigation costs do not confer standing.

II. The Question Presented Is Important.

The overbroad approach to standing in data breach cases reflected in the decision below not only conflicts with this Court's precedents: it will, if permitted to stand, have deeply troubling consequences for both businesses and the federal courts.

A. The Court of Appeals' Approach Would Create Serious And Recurrent Problems For Legitimate Businesses.

Data breaches are an increasingly commonplace—and unavoidable—fact of life in the digital age. "Ultimately, any organization is fair game for cyber threat actors." Council of Economic Advisers, *The Cost of Malicious Cyber Activity* 5 (Feb. 2018), bit.ly/2KeJyXT. Defending successfully against all of these attackers all of the time simply is not possible. See, *e.g.*, Verizon, 2018 Data Breach Investigations Report 10 (2018), bit.ly/2OFJKm6 ("Let's get the obvious and infeasible goal of 'Don't get compromised' out of the way.").

Indeed, one leading study concluded that a typical organization suffers 130 security breaches annually. See Ponemon Institute, *2017 Cost of Cyber Crime Study* 4 (2017), accntu.re/2hsfLik; see also Identity Theft Res. Ctr., *2017 Annual Data Breach Year-End Review* 3 (2018) (describing a 44.7% in-

crease in the number of reported data breaches from 2016 to 2017), bit.ly/2s3TGM9. Breaches can and will occur at any company of any size, and although companies can and do take precautions against such occurrences, a breach is always a possibility despite a company's best efforts to protect its systems.

Data breach litigation, too, is now a fact of life for businesses. The plaintiffs' bar routinely brings suit against businesses whose systems have been attacked by thieves, foreign intelligence services,[4] or other hackers—often within days of a breach being announced. Data breaches are an attractive target for plaintiffs' lawyers because they are widely reported by both the media and the victim companies themselves.[5]

In sum, as one commentator put it, "[i]t's not a question of if you'll be hit with a data breach attempt, but when. And if it's successful, the fallout litigation is just as inevitable." Melissa Maleske, Law360, *The 6 Lawsuits All GCs Face After a Data Breach* (Dec. 9, 2015), bit.ly/2OHEkqr (noting that "[c]onsumer class actions are the most ubiquitous [kind] of post-breach litigation"). Moreover, a single data breach will often give rise to multiple putative

---

[4] See, *e.g.*, Michael Riley & Jordan Robertson, Bloomberg, *Chinese State-Sponsored Hackers Suspected in Anthem Attack* (Feb. 5, 2015), bloom.bg/2NVUpfa.

[5] Every State has a law requiring companies to report data breaches to affected consumers. See, *e.g.*, Nat'l Conf. of State Legislatures, *Security Breach Notification Laws* (Mar. 29, 2018), bit.ly/1ao7NAi ("All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.").

class actions—as demonstrated by the breach at issue here, which led "almost immediately" to multiple actions "in federal district courts across the country." Pet. App. 6.

Permitting suits of this kind to go forward when consumers have not experienced any real-world injury (or a certainly impending one) opens the door to abusive lawsuits, filed to obtain a settlement regardless of the underlying merits of the claim—and very likely to do just that.

The principle applied by the court below does not simply make it easier for plaintiffs to establish standing; it also allows plaintiffs to avoid Rule 23's "stringent requirements for [class] certification." *Am. Express Co.* v. *Italian Colors Rest.*, 570 U.S. 228, 234 (2013). When a plaintiff need not establish any individualized facts to prove standing, it becomes much easier for a putative class to argue that the issues of injury and causation are capable of common proof.

And if such arguments succeed and lead to class certification, settlement may invariably follow: Even when the defendant has strong defenses, putative class actions are virtually never litigated on the merits, because the high stakes exert powerful pressure on the defendant to settle. See, *e.g.*, *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting) ("A court's decision to certify a class . . . places pressure on the defendant to settle even unmeritorious claims."); Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. Rev. 97, 99 (2009) ("With vanishingly rare exception, class certification sets the litigation on a path toward resolu-

tion by way of settlement, not full-fledged testing of the plaintiffs' case by trial.").[6]

Defenders of no-injury data breach litigation sometimes seek to justify these abusive lawsuits on deterrence grounds, claiming they are necessary to hold businesses accountable for data breaches. But that argument fundamentally misunderstands Article III, which focuses on whether the plaintiff has the right to "invoke the authority of a federal court," not on whether particular litigation is thought to serve some desirable purpose. See *DaimlerChrysler Corp.* v. *Cuno*, 547 U.S. 332, 342 (2006). And in any event, the assumption that no-injury data breach litigation is necessary to deter companies from allowing data breaches is wrong, for multiple reasons.

First, enforcing the injury-in-fact requirement does nothing to foreclose plaintiffs who have *actually* been harmed or placed at substantial risk of future harm by a data breach from bringing lawsuits in federal court. In those cases where a data breach can be shown to have caused such harm, consumers can and do hold businesses accountable.

Second, it simply is not credible to suggest that businesses will not take adequate care to prevent data breaches absent no-injury class actions like this one.

To begin with, data security is already heavily regulated under a substantial number of federal and state laws, and public officials frequently bring enforcement actions under those laws. See generally Institute for Legal Reform, *A Perilous Patchwork:*

---

[6] Indeed, *amici* are unaware of any data breach class action that has ever reached trial.

Data Privacy And Civil Liberty In The Era Of The Data Breach (Oct. 2015), bit.ly/2QK8Z85. Federal agencies and state attorneys general have actively pursued companies that have suffered data breaches, requiring "significant penalties and corrective actions" in order to settle their enforcement actions. *Id.* at 11.

For instance, the Federal Trade Commission entered into recent settlements with a technology company[7] and an online tax preparation firm.[8] And in the healthcare context, the Office of Civil Rights (OCR), an agency under the umbrella of the Department of Health and Human Services, "has increased its enforcement efforts" in recent years (*A Perilous Patchwork*, *supra*, at 15), reaching, among other hefty resolutions, a $5.5 million settlement and corrective action plan with a hospital to resolve alleged violations of the Health Insurance Portability and Accountability Act ("HIPAA").[9]

Numerous other state and federal regulators also have brought enforcement actions after data breaches or when they believed that a company's security practices created the risk of such a data breach. See, *e.g.*, U.S. Securities and Exchange Commission, *Altaba, Formerly Known as Yahoo!, Charged With*

---

[7] FTC Press Release, Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims, Apr. 12, 2018, bit.ly/2OC2SRJ.

[8] FTC Press Release, Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules, Aug. 29, 2017, bit.ly/2iZXTeY.

[9] Dep't of Health & Human Servs., Press Release, $5.5 Million HIPAA Settlement Shines Light On The Importance Of Audit Controls, Feb. 16, 2017, bit.ly/2kQGO7h.

Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (April 24, 2018), bit.ly/2HMC4hG; Bureau of Consumer Financial Protection, *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices* (March 2, 2016), bit.ly/2DhpCoT; *A.G. Schneiderman Announces $700,000 Joint Settlement With Hilton After Data Breach Exposed Hundreds Of Thousands Of Credit Card Numbers* (Oct. 31, 2017), on.ny.gov/2ihfj6s.

And businesses have additional, extremely strong incentives to avoid the substantial public relations harm, brand damage, and loss of consumer trust that follows any breach of their customers' data.

Given the already-staggering costs of data breaches,[10] along with the enormous reputational damage they cause, businesses are fully incentivized to invest in reasonable care of the data in their possession without the additional burden of no-injury class actions. Indeed, that is why businesses across industries are investing heavily in cybersecurity and working collaboratively with federal and state governments to protect themselves and their customers from the sophisticated threats they face. See, *e.g.*, Nat'l Inst. of Standards & Tech., *Cybersecurity "Rosetta Stone" Celebrates Two Years of Success* (Feb. 18,

---

[10] See generally Dep't of Justice, *Report of the Attorney General's Cyber Digital Task Force* at xi ("Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families."). As the Chamber's Institute for Legal Reform has reported, "American businesses spend an average of $7.01 million on a single data breach, including the price of notifying potentially affected individuals and ensuing legal costs." Inst. for Legal Reform, *Data Privacy*, bit.ly/2pqXkyE.

2016), bit.ly/2vOEPpo (describing successful cybersecurity risk management framework that resulted from "intensive collaboration with industry" and that has now been widely adopted in the private sector). Requiring businesses to litigate no-injury data breach class actions simply diverts resources that could be used to make these important investments.

In short, the mere occurrence of a data breach should not automatically enable the plaintiffs' bar to launch class-action litigation designed to wrest massive settlements from businesses in the absence of actual harm. This Court's intervention is needed to prevent such abusive litigation.

B. Lower Courts Urgently Require Guidance Regarding The Application Of *Clapper* In The Data Breach Context.

This Court's intervention is also warranted because of the current conflict among courts of appeals on the question presented and the strong likelihood that the legal issues in this case will recur frequently not only in the data breach context but in related factual settings as well.

To begin with, with the law in its current state, most companies are exposed to no-injury data breach litigation, given that most businesses of appreciable size can be sued in one of the five circuits in which the court of appeals has held that the mere fact of a data breach automatically confers standing. This increases legal costs and uncertainty for companies, and acts as a drag on the growing market for "cyber insurance" products that protect against

cybersecurity risks.[11] There is no reason to allow this state of affairs to persist any longer.

Moreover, this Court's guidance would not only bring clarity to data breach litigation; it would also benefit courts faced with consumer litigation involving other types of risks associated with new technologies. In particular, as the "Internet of Things"[12]—*i.e.*, the universe of internet-connected devices and products—has become a significant part of the U.S. economy, businesses producing such products have increasingly become the target of consumer litigation over alleged vulnerabilities in the security systems for those products.

For example, consumers have brought putative class actions over alleged vulnerabilities in internet-connected automobiles[13]; home security systems[14]; children's toys[15]; and medical devices.[16] In cases like

---

[11] See, *e.g.*, Aon Benfield Analytics, *US Cyber Market Update: 2017 US Cyber Insurance Profits and Performance* 2 (July 2018), bit.ly/2OzZkzs (reporting that 170 U.S. insurers offered cyber insurance policies in 2017, up from 140 the previous year, and that total U.S. cyber insurance premiums in 2017 totaled $1.84 billion—"a 37 percent increase from the prior year").

[12] See, *e.g.*, Jacob Morgan, Forbes, *A Simple Explanation Of 'The Internet Of Things,'* (May 13, 2014), bit.ly/2MNSm8n.

[13] See, *e.g., Flynn* v. *FCA US LLC*, 2017 WL 3592040 (S.D. Ill. Aug. 21, 2017); *Cahen* v. *Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Cal. 2015), *aff'd*, 717 F. App'x 720 (9th Cir. 2017).

[14] See *Edenborough* v. *ADT, LLC*, 2016 WL 6160174 (N.D. Cal. Oct. 24, 2016).

[15] See *In re VTech Data Breach Litig.*, 2018 WL 1863953 (N.D. Ill. Apr. 18, 2018).

[16] See Class Action Compl., *Ross* v. *St. Jude Med. Inc.*, No. 2:16-cv-06465 (C.D. Cal. Aug. 26, 2016), ECF No. 1.

these, a key question will be whether a mere allegation that a product contains a cybersecurity vulnerability—without any allegation that malicious actors have exploited or sought to exploit the vulnerability—gives consumers Article III standing.

Though little precedent on that question exists at the moment, it is only a matter of time before courts begin confronting it frequently—and there is a real risk that, absent guidance from this Court, lower courts will divide on the issue in the same way they have on the question presented here. This Court can forestall more splits of authority by taking the opportunity presented by this case to clarify that the fact of a data breach by itself does not confer Article III standing on every consumer whose data is affected.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

STEVEN P. LEHOTSKY
U.S. Chamber Litigation Center
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

STEPHANIE MARTZ
National Retail Federation
1101 New York Ave, NW
Washington, DC 20005
(202) 783-7971

ANDREW J. PINCUS
Counsel of Record
RAJESH DE
STEPHEN C.N. LILLEY
MATTHEW A. WARING
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

SEPTEMBER 2018