No. 25-1895

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

IN RE SAMSUNG ELECTRONICS AMERICA INC.

On Appeal from the United States District Court
for the District of New Jersey, No. 1:23-md-03055-CPO-EAP
Hon. Christine P. O'Hearn

BRIEF FOR THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS *AMICUS CURIAE* IN SUPPORT OF APPELLEE

Jennifer B. Dickey
Kevin R. Palmer
U.S. CHAMBER
LITIGATION CENTER
1615 H Street NW
Washington, DC 20062
(202) 463-5337

Counsel for the Chamber of Commerce of the United States of America

Ashley C. Parrish
Counsel of Record
Megan Michur
KING & SPALDING LLP
1700 Pennsylvania Avenue NW
Suite 900
Washington, DC 20006
(202) 737-0500
aparrish@kslaw.com

Counsel for Amicus Curiae

December 19, 2025

CORPORATE DISCLOSURE STATEMENT

The Chamber of Commerce of the United States of America ("Chamber") states that it is a non-profit, tax-exempt organization incorporated in the District of Columbia. The Chamber has no parent corporation, and no publicly held company has 10% or greater ownership in the Chamber.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

The Chamber of Commerce of the United States of America is the world's largest business federation. It represents approximately 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. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. The Chamber regularly files *amicus curiae* briefs in cases, like this one, that raise issues of concern to the nation's business community.

INTRODUCTION

This case exemplifies the type of improper lawsuit that Article III prohibits. The district court correctly granted Samsung's motion to dismiss because plaintiffs failed to allege an injury in fact. Even though the data breach occurred more than two years ago, plaintiffs have never plausibly alleged that the non-sensitive data at issue — names,

[1] No counsel for any party authored this brief in whole or in part, and no entity or person, aside from *amicus curiae*, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of this brief. The parties have consented to the filing of this brief.

addresses, and product registration identifiers — created "a substantial risk" that stolen data has been or will be misused in a harmful manner. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5, 416 (2013). As the district court explained, "costs incurred to watch for a speculative chain of future events" and fears of hypothetical misuse are not sufficient to confer standing. JA24 (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011)).

The Chamber is submitting this amicus brief to emphasize the importance of the district court's ruling in the digital age and the dangers that would arise if Article III's standing requirements were relaxed in the context of a data-breach class action. Data breaches are an unfortunate fact of life. Businesses, no matter how secure, may find themselves the subject of such a breach. But the vast majority of breaches result in no actual harm to consumers, and they should likewise result in no expensive and burdensome class actions. A proper analysis of Article III helps ensure that only those breaches that result in a concrete injury — and thus a true case or controversy — get into federal court. Breaches involving the disclosure of only non-sensitive information, like this one, do not suffice.

Nor can these breaches satisfy the requirements for class certification under Rule 23 of the Federal Rules of Civil Procedure: Because the risk of harm (if any) from data breaches involving non-sensitive data is both contingent and highly individualized, the proper approach to addressing any issues is on an individualized basis. Allowing class actions, like this one, to proceed on the basis of speculative concerns about remote future injuries would harm businesses and consumers alike and is not a proper use of scarce judicial resources.

Because the district court correctly applied the proper standards, and because plaintiffs have not carried their burden to plead a plausible concrete injury in fact, this Court should affirm.

ARGUMENT

I. Enforcing Article III's standing requirement is important when plaintiffs bring litigation in response to a data breach.

Standing is a constitutional guardrail that ensures that courts resolve concrete disputes and do not step outside the proper judicial role to make policy judgments over generalized risks or abstract grievances. As the Supreme Court has emphasized, "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual

cases or controversies." *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 37 (1976). That principle is especially important where information is taken in an unlawful data breach, and there is a temptation to involve the courts in resolving concerns about speculative harms that may never materialize.

A. Article III requires plaintiffs to carry their burden to demonstrate a concrete, non-speculative injury.

1. The "'irreducible constitutional minimum'" of Article III standing requires each plaintiff to have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992))). All three elements are constitutionally compelled, *see Lujan*, 504 U.S. at 560-561, but the injury-in-fact requirement is "[f]irst and foremost" among them, *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 (1998). To establish an injury in fact, a plaintiff must identify an injury that is "particularized," meaning that it "must affect the plaintiff in a personal and individual way." *Lujan*, 504 U.S. at 560 n.1. The plaintiff also must demonstrate that the injury is "concrete," meaning that it must be "distinct and palpable, as opposed to

merely abstract," *Knudsen v. Metlife Grp., Inc.*, 117 F.4th 570, 577 (3d Cir. 2024) (quotation marks omitted), and "actual or imminent, not conjectural or hypothetical." *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560)).

The burden of establishing Article III standing rests with the party seeking to invoke federal jurisdiction. *See Summers v. Earth Island Inst.*, 555 U.S. 488, 493 (2009). A court must "presume" that jurisdiction is lacking "unless the contrary appears affirmatively from the record." *In re Johnson & Johnson Talcum Powder Prods. Mktg., Sales Pracs. & Liab. Litig.*, 903 F.3d 278, 288 (3d Cir. 2018) (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 342 n.3 (2006)).

The Constitution's injury-in-fact requirement ensures that federal courts exercise "their proper function in a limited and separated government" — adjudicating concrete disputes, not abstract questions of policy. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (quoting John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 Duke L.J. 1219, 1224 (1993)); *see also Allen v. Wright*, 468 U.S. 737, 752 (1984) ("the law of Art. III standing is built on a single basic idea — the idea of separation of powers"). Courts are not authorized to issue advisory

opinions or exercise "general legal oversight" over the conduct of other branches or private entities. *TransUnion*, 594 U.S. at 423; *see also Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 166 (1803). Relaxing the injury-in-fact requirement opens courts to adjudicating hypothetical questions for massive numbers of people, diverting scarce judicial resources to resolve disputes that are beyond the judiciary's proper role. *See Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 474-75 (1982).

2. Article III's mandate that plaintiffs demonstrate a concrete and particularized injury is important in the data breach context. In today's digital age, "hacking attacks are a fact of life." Edward H. Klees, *The "Fandation" of Risk: Does a Banking Client Get Its Money Back After Cyber Theft?*, Bus. L. Today 1 (2016). "[S]mall businesses are targeted by cyberattacks roughly every 11 seconds, while larger enterprises face more than 1,900 attempted attacks each week." Emily Bonnie, *Biggest Data Breaches of 2025: Common Attack Vectors and How to Protect Your Business in 2026*, SecureFrame (Dec. 16, 2025), https://secureframe.com/blog/top-data-breaches-2025. By 2016, almost a decade ago, more than 75% of American companies had already suffered at least one data

breach. Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. Cal. L. Rev. 683, 685 (2017). And nearly two-thirds of American adults had "experienced or been notified of a significant data breach pertaining to their personal data or accounts." Kenneth Olmstead & Aaron Smith, Pew Rsch. Ctr., Americans and Cybersecurity 8 (2017). In the last decade, these numbers have continued to increase. *See Annual number of data compromises and individuals impacted in the United States from 2005 to 2024*, Statista (2025), https://tinyurl.com/4khx7ked.

Although exposure to a data breach may unfortunately be an inevitable fact of modern life, injury from a data breach is not. Most breaches cause no concrete harm. *See* Michael A. Turner et al., Data Flows, Technology, & The Need for National Privacy Legislation 37 (2019), *available at* https://www.uschamber.com/technology/data-flows-technology-the-need-national-privacy-legislation. Proper system design prevents access to sensitive data, and prompt detection and notification can undercut the likelihood of any harm. As a result, only a small fraction of data breaches ever lead to actual consumer harm, like identity theft or fraud. *See In re SuperValu, Inc.*, 870 F.3d 763, 770-71 (8th Cir.

2017). It therefore comes as no surprise that in data breach cases plaintiffs are often able to allege only "mere conjecture about possible" harm by third parties — a scenario that is the very essence of "conjectural or hypothetical." *Clapper*, 568 U.S. at 420; *Lujan*, 504 U.S. at 560.

3. Applying these principles, two points are clear: *First*, mere disclosure of non-sensitive data on its own does not give rise to a concrete injury that satisfied Article III's essential requirements. *TransUnion*, 594 U.S. at 417 ("No concrete harm, no standing."). Concrete injury requires a real-world consequence, and access to basic data (such as names, addresses, product registration information) does not on its own permit identity or financial fraud. Any risk tied to the breach of that data is thus attenuated because harm depends on multiple, additional speculative actions.

As this Court explained in *Reilly v. Ceridian Corp.*, "allegations of hypothetical, future injury are insufficient to establish standing," because any harm "[depends] on entirely speculative, future actions of an unknown third-party" and "on the skill and intent of the hacker." 664 F.3d at 42, 45. Treating data breaches as actionable per se would collapse

the injury requirement into a generalized grievance predicated on "data exposure." *See Baysal v. Midvale Indem. Co.*, 78 F.4th 976, 980 (7th Cir. 2023) (holding that disclosure of driver's-license number does not support standing because it is a "neutral fact derived from a public records system, a fact legitimately known to many private actors and freely revealed to banks, insurers, hotels, and others"); *see also Georgine v. Amchem Prods., Inc.,* 83 F.3d 610, 636 (3d Cir. 1996) (Wellford, J., concurring) ("Fear and apprehension about a possible future physical or medical consequence ... is not enough to establish an injury *in fact*."). The Supreme Court rejected similar arguments in *TransUnion*, holding that "the mere risk of future harm, standing alone, cannot qualify as a concrete harm — at least unless the exposure to the risk of future harm itself causes a separate concrete harm." 594 U.S. at 436 (emphasis omitted).

Second, self-imposed costs and voluntary expenditures are not sufficient to give rise to a concrete injury sufficient to confer standing. Plaintiffs cannot "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Clapper*, 568 U.S. at 416; *see also Baysal*, 78 F.4th at 977 (noting that the cost of

a credit-monitoring service, like other forms of "worry and anxiety," are "not the kind of concrete injury essential to standing"). In *Clapper*, the Supreme Court rejected plaintiffs' argument that costs incurred to avoid speculative harm could establish standing: The "harm" they spent time and money seeking to avoid was speculative, "not certainly impending." 568 U.S. at 416. Likewise, "costs incurred to watch for a speculative chain of future events … are no more 'actual' injuries than the alleged 'increased risk of injury.'" *Reilly*, 664 F.3d at 46; *see also Beck v. McDonald,* 848 F.3d 262, 276 (4th Cir. 2017) (rejecting standing based on credit monitoring and other protective measures taken "in response to a speculative threat" following theft of a laptop and pathology reports containing personal data (quoting *Clapper*, 568 U.S. at 416)). Accordingly, time and money spent monitoring accounts or prophylactic measures like changing passwords or implementing security freezes after a data breach are not sufficient to establish a concrete injury for purposes of Article III standing.

B. The District Court properly dismissed this case for lack of Article III standing.

The district court properly relied on this Court's decision in *Reilly* and dismissed this case, finding that after four attempts plaintiffs failed

to meet their burden. The district court's decision is correct and consistent with other cases where courts recognize that speculative risks are not concrete injuries sufficient to establish Article III standing.

In *Georgine v. Amchem Products*, for example, this Court held that "exposure-only" asbestos plaintiffs lacked standing despite a statistically increased risk of developing disease, because fear and apprehension about future consequences do not constitute a concrete injury. 83 F.3d at 617, 627-28. Although *Georgine* involved latent health risks, it reflects the same constitutional principle: speculative harm cannot substitute for a present and certainly impending injury. Similarly, in *Dinerstein v. Google, LLC,* the Seventh Circuit rejected claims premised on a "risk of future reidentification" of anonymized medical records, explaining that such allegations rested on a chain of hypotheticals rather than any imminent misuse. 73 F.4th 502, 515 (7th Cir. 2023).

Plaintiffs argue that the three non-exhaustive factors set forth in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152-53 (3d Cir. 2022), demonstrate why a breach creates a "substantial risk" of harm, pointing to the alleged intentional nature of the attack, speculative references to misuse, and the types of data accessed. But none of that is sufficient to

identify any actual injury suffered by any individual plaintiff. *See id.* at 153-54. As *Clemens* itself recognized, a "'possible future injury' — even one with an 'objectively reasonable likelihood' of occurring — is not sufficient" to satisfy Article III's requirements. *Id.* at 153 (quoting *Clapper*, 568 U.S. at 409-10, 414 n.5). Article III requires a concrete injury, not just a framework for assessing the potential for elevated risk.

Plaintiffs claim that they plausibly alleged an injury in fact, but they conspicuously fail to identify any evidence of actual injury. The harms they allege — and specifically their claim that they are at risk of identity fraud and theft — are the same speculative, non-concrete harms that any individual subject to a data breach could allege. Applying *Clemens*, the district court properly concluded that, even though plaintiffs plausibly alleged that Samsung was the target of an intentional data breach, there were no plausible allegations that the information had been held for ransom, fraudulently used, or mass published. Most importantly, there are no plausible allegations that the breach resulted in the hackers gaining access to information that is the type of information that subjects an individual to a heightened risk of identity theft. Nor are there plausible allegations linking any fraudulent charges

to the data breach itself. *See* Turner et al., Data Flows, Technology, & The Need for National Privacy Legislation at 38 (noting that "most known cases of fraud occur through traditional methods" and that a survey showed that only 11% of victims reported that improperly accessed information came from a data breach).

In addition, the district court correctly recognized that the mere exposure of non-sensitive data is not a concrete injury sufficient to support a theory of economic loss. Plaintiffs argue that the data breach has prevented them from selling their information or controlling how it is used, purportedly depriving them of the benefit of their bargain with Samsung. But this Court — and others — have rejected such arguments, explaining that an alleged injury is insufficient when it consists solely of buyer's remorse of hypothetical risk without any concrete, measurable harm. For example, in *Johnson & Johnson*, the plaintiff alleged that she would not have purchased talc-based baby powder had she known of an increased risk of ovarian cancer. 903 F.3d at 281. This Court rejected this theory because the plaintiff admitted that the product performed as expected and she did not allege any physical injury, premium price, or diminished value. *Id.* As the Court explained, "buyer's remorse, without

more, is not a cognizable injury under Article III" and mere assertions that she "would not have purchased" the product were insufficient because they did not show any objective economic loss. *Id.* at 281-82; *see also Koronthaly v. L'Oreal USA, Inc.*, 374 F. App'x 257, 258-59 (3d Cir. 2010) (no standing because the plaintiff alleged only that she would not have purchased lipstick containing trace lead, but conceded the product worked as intended and caused no harm).

There is no reason this Court should depart from this well-reasoned precedent. Allowing mere mitigation costs to suffice to establish concrete injury would invite plaintiffs to engage in strategic spending to manufacture jurisdiction, undermining the injury requirement and opening the floodgates to litigation untethered to real-world harm. As *TransUnion* concluded: "Federal courts do not possess a roving commission to publicly opine on every legal question. … [They] resolve only 'a real controversy with real impact on real persons.'" 594 U.S. at 423-24. (quoting *Am. Legion v. Am. Humanist Ass'n*, 588 U.S. 29, 87 (2019) (Gorsuch, J., concurring in the judgment)).

II. Rule 23's requirements ensure that federal courts do not entertain class actions that rely on speculative claims that unravel into individualized inquiries.

Plaintiffs' failure to allege a concrete injury is compounded by their attempt to litigate this case as a putative class action. Rule 23's safeguards reinforce Article III requirements to ensure that federal courts do not allow a case to proceed as a class action when unnamed class members suffer only speculative injuries that cannot be proven except on an individualized basis.

A. "The class action is 'an exception to the usual rule that litigation is conducted by and on behalf of'" individual named parties. *Comcast Corp. v. Behrend*, 569 U.S. 27, 33 (2013) (quoting *Califano v. Yamasaki*, 442 U.S. 682, 700-01 (1979)). To fall within this exception, a plaintiff must satisfy all of Rule 23's requirements by a preponderance of evidence. *In re Hydrogen Peroxide Antitrust Litig.*, 552 F.3d 305, 316, 326 (3d Cir.), *as amended* (Jan. 16, 2009) (noting that courts must conduct a "rigorous analysis," not rely on "bare allegation" (quotation marks omitted)). Rule 23(b)(3)'s "demanding" predominance requirement mandates that a proposed class must be "sufficiently cohesive to warrant adjudication by representation." *Amchem Prods.,*

Inc. v. Windsor, 521 U.S. 591, 623-24 (1997). That cohesion exists only when all class members "possess the same interest and suffer *the same injury*." *E. Tex. Motor Freight Sys., Inc. v. Rodriguez*, 431 U.S. 395, 403 (1977) (emphasis added) (quoting *Schlesinger v. Reservists Comm. to Stop War*, 418 U.S. 208, 216 (1974)). Similarly, to avoid a class action that sweeps in unnamed parties who have not suffered any cognizable injury, Rule 23 requires that a class must be "currently and readily ascertainable based on objective criteria." *Marcus v. BMW of N. Am., LLC*, 687 F.3d 583, 592-93 (3d Cir. 2012) (explaining that subjective injuries are not sufficient).

The need to prove a common, class-wide injury is essential to ensuring "sufficient unity so that absent members can fairly be bound by decisions of class representatives." *Amchem*, 521 U.S. at 620–21. Indeed, in "an era of frequent litigation — and especially "class actions" — "courts must be more careful to insist on the formal rules of standing, not less so." *Ariz. Christian Sch. Tuition Org. v. Winn*, 563 U.S. 125, 146 (2011). When Rule 23(b)(3)'s predominance requirement is not satisfied, including because a class includes uninjured class members, there is nothing to be gained by class certification, "except the blackmail

value of a class certification that can aid the plaintiffs in coercing the defendant into a settlement." *Rutstein v. Avis Rent-A-Car Sys., Inc.*, 211 F.3d 1228, 1240 n.21 (11th Cir. 2000).

B. Plaintiffs' failure here to establish an injury in fact shows why this case also fails to meet the pleading requirements to proceed as a class action. When injury depends on a conjectural chain of events, predominance collapses: courts cannot resolve whether any individual suffered a concrete harm without conducting mini trials on whether any alleged misuse is traceable to this particular breach rather than other incidents, and whether any harm occurred at all.

The Eleventh Circuit's decision in *Cordoba v. DIRECTV, LLC* is illustrative. *See* 942 F.3d 1259 (11th Cir. 2019). In *Cordoba*, plaintiffs alleged that DIRECTV violated the Telephone Consumer Protection Act by making telemarketing calls to individuals on the national Do-Not-Call registry. The proposed class included thousands of people who had received calls, but many of those putative class members had suffered no statutory injury because they had consented to calls or never registered properly. The court explained that determining who had standing would require individualized inquiries into each person's consent history and

call records — questions that could not be resolved with uniform proof. The need for mini trials meant that common issues did not predominate. *See id*. at 1273-75.

The same logic applies here. In data breach cases, injury turns on highly individualized facts. As the district court's findings confirm, only four of 41 named plaintiffs claimed their data appeared on the dark web, and even those allegations lacked specificity and were not sufficient to demonstrate a concrete injury. Thirteen had prior identity-theft incidents unrelated to this breach. Others alleged phishing or hacked accounts without plausible linkage. These variations show why the absence of standing renders it impossible for common issues to predominate. Indeed, plaintiffs' theories of harm — "increased risk," "time spent," and "emotional distress" — vary dramatically from individual to individual and they cannot be proven with common evidence. Those individualized inquiries overwhelm any common questions about Samsung's security practices.

C. Plaintiffs' proposed class also fails the ascertainability requirement, which demands that a class be "currently and readily ascertainable based on objective criteria." *Marcus*, 687 F.3d at 593; *Byrd*

v. Aaron's Inc., 784 F.3d 154, 163 (3d Cir. 2015). Ascertainability requires objective criteria and a feasible mechanism to identify class members. Where injuries are speculative, those criteria do not exist. In *Marcus*, this Court rejected a class definition that required "'mini trials'" to determine whether each tire had "gone flat and been replaced," emphasizing that ascertainability cannot rest on conjecture. 687 F.3d at 593-94. In *Byrd*, this Court clarified that plaintiffs must show class members *can* be identified through reliable records, not by self-identification or hypothetical harm. 784 F.3d at 163-65.

As the district court found, plaintiffs here alleged only "future, hypothetical risk" and harms "dependent on entirely speculative, future actions of an unknown third party," such as phishing or SIM swapping, which require a "highly attenuated chain of possibilities." JA11, JA17, JA22 (quoting *Clemens*, 48 F. 4th at 153; *Reilly*, 664 F.3d at 42; *Clapper*, 568 U.S. at 410)). The information accessed — names, addresses, demographic data, and IMEI numbers — is "not sensitive enough to give rise to an imminent risk of identity theft or fraud," and plaintiffs cannot plausibly link any alleged misuse to this breach. *See* JA18-19, JA23. Without concrete injury, there is no objective marker to determine who

belongs in the class; membership would hinge on subjective fears and unverifiable assertions. As in *Marcus*, that would necessitate individualized inquiries, and unlike *Byrd*, there are no business records or other reliable means to identify affected individuals. Accordingly, the speculative nature of plaintiffs' alleged harm renders the proposed class not ascertainable under this Court's controlling precedent.

III. There are strong policy reasons to enforce essential standing and class action requirements.

Exposure to a data breach is an unfortunate fact of life in our increasingly digital world. But most breaches never lead to identity theft or financial harm. The gap between breach notifications and actual harm is widening, making decisions that treat mere exposure as actionable increasingly detached from real-world outcomes. Treating every breach as actionable — regardless of whether it causes concrete injury — diverts resources from prevention to litigation.

Empirical evidence confirms that most breaches never lead to identity theft or financial harm, even when data is posted online. The Government Accountability Office has found that data breaches are frequent, but evidence of resulting identity theft is "limited," with fewer than three percent of breach victims ever experiencing identity theft.

GAO No. 07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown 29 (June 2007). Similarly, the Chamber's own research confirms that individuals involved in breaches "are not at an especially high risk for ID theft or fraud." Turner et al., Data Flows, Technology, & The Need for National Privacy Legislation at 37 (suggesting a risk of "perhaps one in a thousand, as suggested by" a regression analysis). Even when data appears on the dark web, studies show no practical difference in risk compared to consumers whose data was never breached. *Id*. Litigation experience tells the same story: even years after a breach, plaintiffs routinely fail to show misuse tied to the incident.

Plaintiffs argue that the mere presence of data on the dark web establishes injury. But courts and studies agree that benign data rarely leads to identity theft. *See SuperValu*, 870 F.3d at 770-71; GAO No. 07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited, *supra*. The risk of even potential future injury harm is very low when the data does not include sensitive information such as Social Security numbers or bank account details.

This case demonstrates the point: two years after the breach, plaintiffs have managed to identify a grand total of four individuals who even claim their information was misused as a result of the breach.

Dismissing this improper litigation is also important to avoid abuse of the class action process. *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011) (discussing risks of allowing meritless claims to proceed). As the Supreme Court has warned, "even a complaint which by objective standards may have very little chance of success at trial has a settlement value to the plaintiff out of any proportion to its prospect of success at trial." *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 740 (1975). That dynamic imposes staggering costs: class-action litigation cost U.S.-based companies $3.9 billion in 2023 and $4.2 billion in 2024. *See* Carlton Fields, 2025 Class Action Survey 6-7 (2025) (projecting spending to exceed $4.53 billion in 2025). Defending a single class action can run into nine figures and drag on for years. *See* John H. Beisner et al., U.S. Chamber of Com. Inst. for Legal Reform, Unfair, Inefficient, Unpredictable: Class Action Flaws and the Road to Reform 15, 36 (2022). These costs are inevitably passed on to consumers through higher prices and reduced investment in security, meaning "to the extent there are any

winners in class actions, they are not consumers." *Id.* at 26. Such litigation also creates perverse incentives: companies that respond effectively to prevent harm — like Samsung did — would still face years of costly litigation, despite no actual injury to customers. These suits do not compensate victims; they punish businesses for being hacked by diverting their revenues to class action attorneys.

Because data breaches that expose only non-sensitive information do not result in concrete injury (and certainly cannot be assumed to cause injury on a class-wide basis), the proper vehicle to address alleged harm is through individualized litigation. Enforcing the injury-in-fact requirement does not bar plaintiffs who have suffered actual harm from pursuing those claims in federal court. It appropriately marshals and reserves judicial resources for the true cases or controversies.

CONCLUSION

For these reasons, the Court should affirm the judgment below.

Respectfully submitted,

s/ Ashley C. Parrish

Jennifer B. Dickey
Kevin R. Palmer
U.S. CHAMBER
LITIGATION CENTER
1615 H Street NW
Washington, DC 20062
(202) 463-5337

Counsel for the Chamber of Commerce of the United States of America

Ashley C. Parrish
Counsel of Record
Megan Michur
KING & SPALDING LLP
1700 Pennsylvania Avenue NW
Suite 900
Washington, DC 20006
(202) 737-0500
aparrish@kslaw.com

Counsel for Amicus Curiae

December 19, 2025

CERTIFICATE OF COMPLIANCE

1. Pursuant to Local Rule 28.3(d), I hereby certify that I am a member of the bar of this Court.

2. This brief complies with the type-volume requirements of Federal Rules of Appellate Procedure 29(a)(5) because it contains 4,534 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f).

3. The brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) and 3d Cir. L.A.R. 32.1(c) because it has been prepared in a proportionally spaced typeface using Microsoft Word 365 ProPlus in Century Schoolbook 14-point font.

4. Pursuant to Local Rule 31.1(c), I hereby certify that the text of the electronic brief is identical to the text in the paper copies, and that it has been scanned for viruses using Microsoft Defender and no virus was detected.

Dated: December 19, 2025

s/ Ashley C. Parrish
Ashley C. Parrish
Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that on December 19, 2025, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the CM/ECF system. I certify that all participants in the appeal are registered CM/ECF users and service will be accomplished by the CM/ECF system.

s/ Ashley C. Parrish
Ashley C. Parrish
Counsel for Amicus Curiae