No. 25-

IN THE

Supreme Court of the United States

ELEPHANT INSURANCE COMPANY;
ELEPHANT INSURANCE SERVICES, LLC;
PLATINUM GENERAL AGENCY, INC.
D/B/A/ APPARENT INSURANCE,

Petitioners,

v.

CHRISTOPHER HOLMES; TRINITY BIAS;
JAIME CARDENAS; AND ROBERT SHAW,
INDIVIDUALLY AND ON BEHALF OF ALL
OTHERS SIMILARLY SITUATED, *et al.*,

Respondents.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

CLAUDIA D. MCCARRON
Counsel of Record
MULLEN COUGHLIN LLC
426 West Lancaster Avenue,
Suite 200
Devon, PA 19333
(267) 930-4770
cmccarron@mullen.law

Attorney for Petitioners

391134

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

QUESTIONS PRESENTED

1. The Court has held that a plaintiff can establish Article III standing through an intangible injury-in-fact where (1) that injury bears a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts and (2) that injury includes the elements "essential to liability" in a suit for that harm. The first question presented is whether it is "essential to liability" that the defendant—and not a third party—commit the act giving rise to the injury that bears the close relationship to the traditionally recognized harm.

2. The United States Courts of Appeals for the Fourth Circuit and for the Seventh Circuit have split over whether the publication of personal information that is neither embarrassing nor sensitive is sufficiently analogous to the common law harm of public disclosure of private facts to confer Article III standing. The second question presented is whether a plaintiff can establish Article III standing through analogy to public disclosure of private facts when the information is neither embarrassing nor sensitive.

PARTIES TO THE PROCEEDINGS

Petitioners, who were Defendants-Appellees below, are Elephant Insurance Company; Elephant Insurance Services, LLC; and Platinum General Agency, Inc., doing business as Apparent Insurance.

Respondents, who were Plaintiffs-Appellants below, are Christopher Holmes; Trinty Bias; Jaime Cardenas; and Robert Shaw, individually and on behalf of all others similarly situated.

RULE 29.6 STATEMENT

Petitioner Platinum General Agency, Inc., is a wholly owned subsidiary of Petitioner Elephant Insurance Services, LLC. Petitioner Elephant Insurance Services, LLC, is a wholly owned subsidiary of Elephant Holding Company, LLC. Petitioner Elephant Insurance Company is a wholly owned subsidiary of Elephant Holding Company, LLC.

Elephant Holding Company, LLC, has the following parent companies: Brick Holdings BidCo, LLC; Brick Holdings MidCo, LLC; Brick Holdings ParentCo, LLC; Brick Holdings TopCo L.P.; JCF Associates VI L.P.; and JCF Associates VI Ltd. JCF Associates VI Ltd. is the ultimate parent company of all Petitioners. No publicly held company owns 10 percent or more of any of the Petitioners' stock.

STATEMENT OF RELATED PROCEEDINGS

This case is currently proceeding in the United States District Court for the Eastern District of Virginia, Case No. 3:22-cv-487.

TABLE OF CONTENTS

Table of Contents

TABLE OF APPENDICES

TABLE OF CITED AUTHORITIES

Page

Cases

Page

Statutes and Other Authorities

Page

PETITION FOR A WRIT OF CERTIORARI

Petitioners Elephant Insurance Company; Elephant Insurance Services, LLC; and Platinum General Agency, Inc., doing business as Apparent Insurance (collectively "Elephant"), respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Fourth Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (App. 1a-38a) is reported at 156 F.4th 413. The order of the district court (App. 39a-54a) granting defendants' motion to dismiss plaintiffs' complaint is available at 2023 WL 4183380.

The judgment of the court of appeals was entered on October 14, 2025. The Court's jurisdiction rests on 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

Article III, Section 2 of the U.S. Constitution provides that "[t]he judicial Power shall extend to all Cases, in Law and Equity, arising under * * * the Laws of the United States * * *."

STATEMENT OF THE CASE

Each year, an increasing number of data breach class actions inundate the federal courts. The nature of data breaches are such that most impacted people suffer no tangible harm traceable to that specific incident. As a result, plaintiffs are often left to allege intangible injuries

such as loss of privacy, risk of future identity theft, and emotional distress. At the forefront of these cases is the question of what a plaintiff must show to establish a concrete injury-in-fact for standing under Article III of the Constitution. In the five years since the Court's decision in *TransUnion, LLC v. Ramirez*, 594 U.S. 413 (2021), the lower federal courts have yet to settle on a consistent standard in determining Article III standing in data breach cases in which the named plaintiffs have not suffered identity theft or other concrete harms that are traceable to the underlying data security incident.

The decision of the U.S. Court of Appeals for the Fourth Circuit is emblematic of this muddled landscape. Deviating from the other circuit courts that have addressed the Court's analogous harm concept articulated in *TransUnion*, the Fourth Circuit found that a plaintiff can establish Article III standing by analogy to a common law tort even where an essential element of that tort—that the defendant committed it—is missing. Specifically, the court of appeals found that a data breach plaintiff can demonstrate standing at the pleading stage by alleging that a criminal hacker—and not the defendant—published the plaintiff's driver's license number on the dark web.[1] The Fourth Circuit held that this alleged injury was sufficiently analogous to the common law harm of public

1. "The Dark Web is a general term that describes hidden Internet sites that users cannot access without using special software." *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3dd 295, 302 n.4 (2d Cir. 2021) (citing Kristin Finklea, Cong. Rsch. Serv., 7-5700, *Dark Web* 2 (2017)) (internal quotation marks omitted). Contrary to the Fourth Circuit's opinion, it is not "a forum accessible to all—or at least to those with some degree of proficiency with computers." App. 18a.

disclosure of private facts "even if the situation was brought about through no fault or action of the defendant." App. 19a. The Fourth Circuit's decision misconstrues the Court's Article III standing jurisprudence and splits with how other circuit courts have addressed that Article III analogous harm analysis.

Under the Court's precedent, plaintiffs "must demonstrate standing for each claim that they press against each defendant." *Murthy v. Missouri*, 603 U.S. 43, 61 (2024) (quoting *TransUnion*, 594 U.S. at 431) (internal quotation marks omitted). In data breach cases, plaintiffs are almost never able to find and sue the criminal hacker responsible for the breach. They instead seek damages from the hacked entity for allegedly employing insufficient data security practices. When analogizing an intangible privacy injury to one protected at common law, whether the defendant—and not a criminal hacker who stole data from that defendant—was the actor who brought about the specific harm is "essential to liability." *TransUnion*, 594 U.S. at 434. Here, there is no question that the criminal hacker was the party that made the disclosure on the dark web. Ignoring that essential element, the Fourth Circuit's decision allows a plaintiff to demonstrate standing *against a defendant* by analogizing an intangible privacy injury to a common law harm *committed by someone other than that defendant*. No other circuit court has found that a plaintiff can establish Article III standing by analogizing the alleged injury to a common law harm where "the situation was brought about through no fault or action of the defendant." App. 19a. The Fourth Circuit's holding "circumvents a fundamental requirement of" the analogous tort—that the defendant is the one who committed it. *TransUnion*, 594 U.S. at 434 n.6.

The Fourth Circuit also found that it was immaterial to its analysis that driver's license numbers are not the type of embarrassing or sensitive information traditionally protected under the tort of public disclosure of private facts. Despite noting that people "do not consider their driver's licenses embarrassing and hand them to bartenders and waiters and police officers without hesitation," the court of appeals noted that *TransUnion* only required "harms that are analogues, not duplicates." App. 20a-21a. The Fourth Circuit recognized that this holding created a direct conflict with the Seventh Circuit. *Id.* Addressing the identical question in a data breach class action, the Seventh Circuit found that the publication of driver's license numbers on the dark web was insufficiently analogous to public disclosure of private facts because a driver's license number 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." *Baysal v. Midvale Indem. Co.*, 78 F.4th 976, 980 (7th Cir. 2023). The Seventh Circuit's analysis recognizes that the embarrassing or sensitive nature of the information is an element "essential to liability" for public disclosure of private facts and is missing when the information is a driver's license number.

Given the proliferation of data breach class actions in recent years, this circuit split places defendants located within the Fourth Circuit at a distinct disadvantage compared to defendants located within the Seventh Circuit, as plaintiffs in the Fourth Circuit are now far likelier to demonstrate Article III standing at the pleading stage. For many plaintiffs within the Fourth Circuit, clearing the standing threshold becomes no challenge at all, because all they need to show is that some piece of

non-sensitive personal information was published on the dark web "through no fault or action of the defendant." App. 19a.

The growing wave of data breach class actions shows no sign of slowing down. Now that the Fourth Circuit has made it far easier for plaintiffs to demonstrate Article III standing, it is even more likely to speed up. As these matters continue to fill up the federal court dockets, this case presents an ideal vehicle for the Court to clarify whether a plaintiff must plead facts showing all elements "essential to liability" when demonstrating Article III standing through analogy to a harm traditionally recognized at common law.

a. Factual Background and District Court Proceedings

Elephant is an insurance company that sells automobile and other types of insurance products. In the course of providing insurance products, Elephant comes into possession of various types of personal information from customers and potential customers. Between March 26 and April 1, 2022, cybercriminals unlawfully accessed Elephant's computer network and copied certain data. The hackers potentially accessed Respondents' names, birth dates, and driver's license numbers. Elephant provided notice to 2,762,687 individuals that their information may have been affected.

Respondents sued Elephant shortly after receiving notice of the incident and filed their consolidated complaint in the U.S. District Court for the Eastern District of Virginia on September 14, 2022, asserting causes of action for violation of the Driver's Privacy Protection

Act, negligence, negligence *per se*, unjust enrichment, violation of the Texas Consumer Protection Act, violation of the Illinois Consumer Privacy Act, violation of the Illinois Uniform Deceptive Trade Practices Act, and declaratory and injunctive relief. Although Respondents Jaime Cardenas and Christopher Holmes alleged that they had received notifications from credit monitoring services that their driver's license numbers had been found on the dark web, none of the four Respondents alleged identity theft or other concrete harm stemming from the incident.

Elephant moved to dismiss the complaint on October 14, 2022, and the district court granted that motion on June 26, 2023, finding that Respondents failed to plead injuries-in-fact fairly traceable to the data security incident that would give them standing under Article III. The district court held that Respondents could not establish standing through an alleged heightened risk of identity theft, loss of privacy, emotional distress, diminished value of personal information, or mitigative measures. App. 47a-52a. Although Cardenas and Holmes had alleged that their driver's license numbers had appeared on the dark web, the district court found these allegations insufficient to establish standing because Cardenas and Holmes "have not alleged any misuse of their [personal information] or resulting harm from their driver's license numbers appearing on the dark web[.]" App. 49a. Finding that none of the four Respondents had alleged a concrete injury-in-fact fairly traceable to the Elephant data security incident sufficient to demonstrate Article III standing, the district court granted the motion to dismiss for lack of subject matter jurisdiction.

b. The Fourth Circuit's Opinion

The Fourth Circuit affirmed in part and reversed in part the district court's decision.

The court of appeals found that Cardenas and Holmes had established Article III standing at the pleading stage because they had alleged that their driver's license numbers had been found on the dark web. App. 18a. For purposes of alleging a concrete injury-in-fact, the Fourth Circuit found that the publication of a driver's license number on the dark web by a criminal hacker was sufficiently analogous to the common law harm of public disclosure of private facts. *Id.* Noting that public disclosure of private facts is one of the four traditional theories for the invasion of privacy tort, the Fourth Circuit explained that this cause of action requires "that *the defendant* (1) disclose (2) to the public (3) true but private information that would be highly offensive to a reasonable person and (4) is otherwise of no legitimate concern to the public." App. 12a (citing Restatement (Second) of Torts § 652D & Special Note & cmt. A; *Cape Publications, Inc. v. Hitchner,* 549 So. 2d 1374, 1377 (Fla. 1989); *Shulman v. Group W Productions, Inc.,* 18 Cal. 4th 200, 74 Cal. Rptr. 2d 843, 955 P.2d 469, 478 (Cal. 1998)) (emphasis added).

The court disagreed with Elephant's argument "that the plaintiffs' theory of concrete injury should fail because they cannot satisfy one element required for liability under the public-disclosure tort: that Elephant made a disclosure." App. 18a-19a. In the Fourth Circuit's view, when analogizing an intangible injury to a common law tort for standing purposes, "the only elements that matter are the ones that define the harm of the analogous

cause of action. A defendant's disclosure, though also *an* element of the public disclosure of private information tort, is not a *harm-defining* element—it goes to the defendant's liability, not to what is felt by the plaintiff." App. 19a (emphasis in original). The court concluded that the harm inflicted *by the criminal hackers* was sufficient for Cardenas and Holmes to establish Article III standing *against Elephant*: "Though the defendant cannot be held liable under the public-disclosure tort without disclosure, there is still a concrete injury." App. 19a-20a. What the court did not address was the fact that the defendant making the disclosure is an element "essential to liability." *TransUnion*, 594 U.S. at 434.

On the question of whether a driver's license number was the type of information that was sufficiently private to be protected under an analogue to public disclosure of private facts, the Fourth Circuit recognized that the Seventh Circuit found that it was not but then noted that "we see things differently." App. 20a. The court began its analysis of this issue by stating, "[u]ndoubtedly, a driver's license number is unlike the details of an affair or a medical condition. People do not consider their driver's licenses embarrassing and hand them to bartenders and waiters and police officers without hesitation." *Id.* The court nevertheless stated that it " cannot accept that a concrete injury exists only if the information publicized is embarrassing." App. 21a. Further, noting that the Seventh Circuit appeared to suggest that Social Security numbers could be considered sufficiently private to be protected, the court concluded that, "[i]f publicizing social security numbers would inflict a kind of concrete injury, we see no reason why driver's license numbers would be different." App. 22a.

Though Cardenas and Holmes had standing to seek damages based on the disclosure of their driver's license numbers on the dark web, the Fourth Circuit found that they did not have standing to seek damages based on any other theory of injury, including increased risk of identity theft. The court also found that Respondents Trinity Bias and Robert Shaw did not have Article III standing on any basis.

This petition followed.

REASONS FOR GRANTING THE PETITION

By finding that a plaintiff can demonstrate Article III standing through analogy to a common law harm even where a third party commits the act resulting in the harm, the Fourth Circuit created two circuit splits.

First, the Fourth Circuit split from all other circuits by finding a plaintiff can establish Article III standing based on an analogy to a harm traditionally protected at common law even when the defendant is not the party committing the act resulting in the analogous harm. Second, as the Fourth Circuit expressly recognized in its opinion, it created a split with the Seventh Circuit on whether the embarrassing and sensitive nature of information is an essential element in finding Article III standing based on an analogy to the tort of public disclosure of private facts.

To establish standing under Article III, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and

(iii) that the injury would likely be redressed by judicial relief." *TransUnion*, 594 U.S. at 423 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–561, (1992)). "If 'the plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve.'" *Id.* (quoting *Casillas v. Madison Avenue Assocs., Inc.*, 926 F.3d 329, 333 (7th Cir. 2019) (Barrett, J.)). When determining whether an asserted injury is concrete, the Court has repeatedly advised courts to "assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 424 (quoting *Spokeo, Inc.* v. *Robins*, 578 U. S. 330, 340 (2016)).

In *TransUnion*, a class of 8,185 individuals brought claims against a credit reporting agency for violation of the Fair Credit Reporting Act because their credit files included alerts from the Treasury Department's Office of Foreign Assets Control erroneously labeling the individuals as potential terrorists. *Id.* at 430. The Court found that only the 1,835 class members whose credit reports the defendant disclosed to third parties had standing. *Id.* at 432. The 6,332 individuals whose reports the defendant did not disclose did not have standing. *Id.* at 437. The Court reached this conclusion by analogizing the asserted intangible injury to the common law harm of defamation. The plaintiffs with undisclosed credit reports could not show the element of publication by the defendant—an element that is "'essential to liability' in a suit for defamation." *Id.* at 435. Although the plaintiffs argued that TransUnion's internal disclosure of the reports was sufficiently analogous to defamation, the Court found that "the plaintiffs' internal publication

theory circumvents a fundamental requirement of an ordinary defamation claim—publication—and does not bear a sufficiently 'close relationship' to the traditional defamation tort to qualify for Article III standing." *Id.* at 434 n.6. Accordingly, in *TransUnion*, the Court clarified that a plaintiff can establish Article III standing based on an intangible harm that has a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts so long as it is not missing an element "essential to liability" or a "fundamental requirement" of that traditionally recognized cause of action.

As the Fourth Circuit explained in this case, the traditional tort of public disclosure of private facts requires that "that *the defendant* (1) disclose (2) to the public (3) true but private information that would be highly offensive to a reasonable person and (4) is otherwise of no legitimate concern to the public." App. 12a (internal citations omitted) (emphasis added). In its decision, however, the Fourth Circuit discarded at least two of the elements essential to liability: (1) that the defendant actually make the disclosure; and (2) that the private information would be highly offensive to a reasonable person. In doing so, the court of appeals "loosen[ed] Article III" in order to find standing based on a claim that does not bear a close relationship to public disclosure of private facts. *TransUnion*, 594 U.S. at 424-425.

Not only did the Fourth Circuit's decision create two circuit splits, but it also resulted in a lowered Article III standing threshold for a category of cases that continues to occupy a larger portion of the federal dockets each year.

a. The Fourth Circuit's Decision Creates a Circuit Split on Whether the Defendant Must Commit the Act Resulting in the Traditionally Recognized Analogous Harm

In finding Article III standing for Cardenas and Holmes at the pleading stage based on an analogy to public disclosure of private facts, the Fourth Circuit stated that "one element required for liability" that did not matter for this analysis was "that Elephant made a disclosure." App. 18a-19a. This is a departure from what the Court prescribed in *TransUnion* and from how other circuit courts have applied that analysis.

In *TransUnion*, the distinguishing factor between the group of plaintiffs who demonstrated Article III standing and the group of plaintiffs who did not was the defendant's publication of the credit reports. *TransUnion*, 594 U.S. at 434. "Publication is 'essential to liability' in a suit for defamation." *Id.* (quoting Restatement of Torts § 577, Comment *a*, at 192). Similarly, in a suit for public disclosure of private facts, it is "essential to liability" that the defendant make the subject disclosure. Despite acknowledging that a defendant's disclosure is "required for liability" under the analogous cause of action, the Fourth Circuit nevertheless found Article III standing without ever explaining how "required for liability" differs from "essential to liability." App. 18a. Had the analogous tort been battery, it would have been illogical to find standing against a defendant who did not make contact with the plaintiff. The same rationale should apply here when seeking Article III standing to proceed against a defendant that made no disclosure.

In explaining its decision, the Fourth Circuit stated that "not all elements of a cause of action go to the harm addressed" and that "elements that pertain to the details of the defendant's action will often—though not always—be unrelated to the kind of harm felt by the victim." App. 10a. In this scenario, the defendant, Elephant, did not take any action that resulted in the harm addressed by public disclosure of private facts. That tort is not suited to deal with alleged negligence in the maintenance of proper data security; rather, it is concerned with disclosure of private information.

In the Fourth Circuit's view, the fact that a criminal third party made the disclosure on the dark web did not "circumvent[] a fundamental requirement of an ordinary" cause of action for public disclosure of private facts. The Fourth Circuit emphasized the need to focus on the harm itself and stated that its "focus on harm over elements is shared by our sister circuits." App. 11a n.7 (citing *Barclift v. Keystone Credit Servs., LLC,* 93 F.4th 136, 145 (3d Cir. 2024) ("*TransUnion* speaks only of harms, not elements."); *Drazen v. Pinto,* 74 F.4th 1336, 1343 (11th Cir. 2023) (en banc) (requiring the presence of "element[s] essential to the harm" in assessing common-law analogues); *Nabozny v. Optio Sols. LLC,* 84 F.4th 731, 734 (7th Cir. 2023) (listing several examples of the types of harm that provide standing); *Shields v. Pro. Bureau of Collections of Md., Inc.,* 55 F.4th 823, 829 (10th Cir. 2022) (stating that the plaintiff "did not have to plead and prove the tort's elements to prevail" but had "to at least allege a similar harm")).

Not a single one of the cases cited by the Fourth Circuit resulted in a court finding Article III standing

based on an analogous harm caused by the action of a third party. In another data breach action, the Second Circuit did find Article III standing based on an analogy to public disclosure of private facts, but in that case, the subject disclosure was the defendant's alleged disclosure of information to the criminal threat actor. *See Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 286 (2d Cir. 2023) ("The core of the injury Bohnak alleges here is that she has been harmed by the exposure of her private information—including her SSN and other PII—to an unauthorized malevolent actor."). The Second Circuit's *Bohnak* case was also wrongly decided but for a separate reason. In *Bohnak*, there was no allegation that either the defendant or the hacker had disclosed any information publicly—an element "essential to liability" for that cause of action—but unlike in this matter, the Second Circuit characterized the defendant as the one making the private disclosure to the hacker. This inconsistent application of the analogous harm test in data breach cases only further underscores the need for clarification from the Court.

The Eleventh Circuit has taken a different approach. Instead of elevating harms over elements, that court found that an examination of all of the elements of the analogous cause of action will reveal whether there is a harm that can confer Article III standing: "When viewed as a way to evaluate whether actual harm occurred, this approach makes sense—if the elements do not match up, how could the harm that results from those elements?" *Hunstein v. Preferred Collection and Mgmt. Servs., Inc.*, 48 F.4th 1236, 1240 (11th Cir. 2022). That is because "when an element 'essential to liability' at common law is missing from an alleged harm, the common-law comparator is not closely related to that harm." *Id.* at 1244 (citing *TransUnion*, 594 U.S. at 434).

An element essential to liability—a disclosure by the defendant—is missing here. The Fourth Circuit has split from its sister circuits in granting Article III standing where the defendant is not the actor causing the analogous harm. The Court should grant this petition to resolve that split.

b. The Fourth and Seventh Circuit Have Split Over Whether the Disclosure of Non-Sensitive and Non-Embarrassing Information Can Serve as a Basis for Article III Standing

Addressing the identical legal issue—whether the publication of driver's license numbers on the dark web is sufficiently analogous to the common law harm of public disclosure of private facts to confer Article II standing in a data breach case—the Fourth and Seventh Circuits have reached opposite conclusions, creating a circuit split.

The two courts agree that driver's license numbers are neither particularly sensitive nor embarrassing. *See* App. 20a ("Undoubtedly, a driver's license number is unlike the details of an affair or a medical condition. People do not consider their driver's licenses embarrassing and hand them to bartenders and waiters and police officers without hesitation."); *Baysal*, 78 F.4th at 979 ("A license number is not viewed as embarrassing (as a low grade point average or a poor credit score would be) or private (as medical details are) but as neutral: most adults have these numbers, which are neither good nor bad.").

For the Seventh Circuit, that was enough to answer the standing question in the negative. *Baysal*, 78 F.4th at 980 ("Plaintiffs have not plausibly alleged that Midvale's

disclosure of their numbers caused them any injury, and the disclosure of a number in common use by both public and private actors does not correspond to any tort."). The Fourth Circuit "[saw] things differently." App. 20a. Noting that the tort "protects some types of information that we would not strictly consider embarrassing," the Fourth Circuit found driver's license numbers to be protected for two reasons. First, pointing out that the Seventh Circuit suggested that Social Security numbers could be protected under this tort, the Fourth Circuit concluded that the difference between Social Security numbers and driver's license numbers was one of degree and not of kind. App. 21a (citing *Baysal,* 78 F.4th at 977, 979). Second, the Fourth Circuit found that Congress's protection of information from a motor vehicle record under the Driver's Privacy Protection Act weighed in favor of finding standing on this basis. App. 22a.

That the disclosure of the private information be highly offensive to a reasonable person is an element essential to liability for public disclosure of private facts. The Fourth and Seventh Circuits have now split over whether the publication of driver's license numbers on the dark web after a data breach bears a close relationship to this harm. The Court should grant the petition to resolve this split.

c. The Questions Presented Are Important, Frequently Recurring, and Cleanly Presented

Plaintiffs filed more than 1,800 data breach class action lawsuits in 2025, which was a 25 percent increase from 2024 and more than a 200 percent increase since 2022. Edward Segal, *Class Action Lawsuit Settlements Set Another Record In 2025*, Forbes, Jan. 6, 2026, https://

www.forbes.com/sites/ edwardsegal/2026/01/06/class-action-lawsuit-settlements-set-another-record-in-2025/.

Given the proliferation of data breach class actions, ensuring that plaintiffs have suffered a concrete injury-in-fact sufficient to demonstrate Article III standing should be a paramount consideration. As the Court has explained, "[i]n an era of frequent litigation [and] 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). As the number of data breach cases has grown, so too has the confusion among the lower courts about how to consider Article III standing when confronted with an array of intangible harms. This case presents the ideal opportunity for the Court to clarify the rules of Article III standing in a constantly growing area of class action litigation.

The Fourth Circuit's decision has lowered by a significant measure the bar that plaintiffs must clear to show Article III standing in a data breach case. Requiring only the mere presence of a non-sensitive personal information to be published on the dark web, the decision opens the doors to dubious claims and forces defendants into settling what may be weak lawsuits. *See AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011) ("When damages allegedly owed to tens of thousands of potential claimants are aggregated and decided at once, the risk of an error will often become unacceptable. Faced with even a small chance of a devastating loss, defendants will be pressured into settling questionable claims.").

The Fourth Circuit's decision in this case has resulted in two circuit splits and has sowed further confusion in

the lower courts' approach to Article III standing in a rapidly expanding area of federal litigation. The Court should take this opportunity to clarify whether a plaintiff must meet all elements essential to liability when seeking to establish Article III standing through analogy to a traditionally protected harm.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Claudia D. McCarron
Counsel of Record
Mullen Coughlin LLC
426 West Lancaster Avenue,
Suite 200
Devon, PA 19333
(267) 930-4770
cmccarron@mullen.law

Attorney for Petitioners

APPENDIX

TABLE OF APPENDICES

APPENDIX A — OPINION OF THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT, FILED OCTOBER 14, 2025

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 23-1782

CHRISTOPHER HOLMES; TRINITY BIAS; JAIME CARDENAS; ROBERT SHAW, INDIVIDUALLY AND ON BEHALF OF THOSE SIMILARLY SITUATED,

Plaintiffs-Appellants,

v.

ELEPHANT INSURANCE COMPANY; ELEPHANT INSURANCE SERVICES, LLC; PLATINUM GENERAL AGENCY INC., d/b/a APPARENT INSURANCE,

Defendants-Appellees.

Appeal from the United States District Court for the Eastern District of Virginia, at Richmond. John A. Gibney, Jr., Senior District Judge. (3:22-cv-00487-JAG)

Argued October 29, 2024 Decided October 14, 2025

Before AGEE, RICHARDSON, and BERNER, Circuit Judges.

Affirmed in part, reversed in part, and remanded by published opinion. Judge Richardson wrote the opinion, in which Judge Agee and Judge Berner joined.

RICHARDSON, Circuit Judge:

Privacy is an endangered species in the digital age. In the day-to-day, we give our personal data to banks and schools, airlines and telecom providers, search engines and e-commerce platforms—and, relevantly, insurance companies. But these third parties are imperfect stewards of our personal information. Some are leaky of their own accord. Others are plundered despite their best efforts. And when they fall short in guarding our information, there are inevitably lawsuits. This is one of those lawsuits.

On appeal before us, however, is solely the limited question of whether the plaintiffs here even *can* bring suit, or whether they lack standing to do so. We hold that a subset of the plaintiffs has standing to continue their suit on one of their alleged injuries-in-fact. We affirm the district court's dismissal of the remainder.

I. BACKGROUND

Elephant Insurance Company, Elephant Insurance Services LLC, and Apparent Insurance (collectively, "Elephant") sell various forms of insurance, including home and car insurance. To make purchasing insurance more convenient, Elephant—like many other insurance providers—designed its online quoting platform to auto-populate certain information like driver's license numbers whenever a potential customer provided other information

such as their name, address, and date of birth. The quoting platform's auto-populate feature was made possible by Elephant's database of personal information, which includes information not just from its own customers but also from third-party sources like DMV records.

Unnamed hackers breached Elephant's network between March 26 and April 1, 2022, compromising the driver's license numbers of nearly 3 million people. Although Elephant has not confirmed how the information was compromised, the plaintiffs allege that the hackers took advantage of Elephant's quoting platform by entering a person's publicly available information and acquiring their driver's license number via the auto-populate feature. Elephant announced the breach in a public statement a month later, sending individualized notices of the breach, along with an offer of a year of free credit monitoring, to all those affected.

Among those affected were Trinity Bias, Jaime Cardenas, Christopher Holmes, and Robert Shaw. In July, a few months after they were notified that their personal information was compromised in the breach, Bias and Cardenas sued Elephant on behalf of a putative class. A few days later, Holmes brought a substantially similar class action. The district court consolidated the two cases, and the parties—now with Shaw—filed a consolidated class action complaint putatively representing all people affected by the breach of Elephant's network. [1]

---

1. The consolidated complaint contains five class-wide claims: (1) a violation of the Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq.*; (2) negligence; (3) negligence *per se*; (4) unjust enrichment; and

Appendix A

In the consolidated complaint, the four plaintiffs asserted that the breach injured them in various ways. All four alleged that they spent time reviewing their credit and financial documents—time they would otherwise have spent on other productive activities. All four also alleged that the breach increased their risk of identity theft, with Cardenas and Holmes claiming that they had found their driver's license numbers on the dark web. Holmes and Shaw added that this risk caused them significant fear, anxiety, and stress. And Holmes alone asserted that he experienced an uptick in texts and calls from spammers requesting his insurance policy information or posing as debt collectors. As relief, the plaintiffs requested monetary damages, a declaration that Elephant's existing security measures are unlawfully inadequate, and an injunction against Elephant ordering it to improve its data security.

The plaintiffs' class action suit never made it past the threshold. Instead, the district court concluded that the plaintiffs lacked standing to pursue any of their claims. *See Holmes v. Elephant Ins. Co.*, 2023 U.S. Dist. LEXIS 110161, 2023 WL 4183380, at *1 (E.D. Va. June 26, 2023). The district court identified and rejected several possible injuries in the plaintiffs' complaint. The district court thus granted Elephant's Rule 12(b)(1) motion as to all plaintiffs

---

(5) declaratory relief under the Declaratory Judgment Act. It also includes three additional claims for two subclasses: (6) a violation of the Texas Consumer Protection Act for the Texas Subclass, Texas Bus. & Com. Code §§17.41 *et seq.*; and (7) a violation of the Illinois Consumer Fraud Act, 815 ILCS §§ 505 *et seq.*; and (8) a violation of the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS §§ 510/2 *et seq.*, both for the Illinois Subclass.

and dismissed the entire case. *2023 U.S. Dist. LEXIS 110161, [WL]* at *6.

The plaintiffs then timely appealed the district court's dismissal.

II. DISCUSSION

The federal courts can only resolve "Cases" and "Controversies." U.S. Const. art. III, § 2, cl. 1. This requires a plaintiff to have a "personal stake"—known as "standing"—in the suit he brings. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423, 141 S. Ct. 2190, 210 L. Ed. 2d 568 (2021). He "must be able to sufficiently answer the question: 'What's it to you?'" *Id.* (quotation omitted). To do so, a plaintiff must show three things: "(i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *Id.* (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992)).

Some plaintiffs may need to answer the standing question more than once. "[S]tanding is not dispensed in gross." *Town of Chester, N.Y. v. Laroe Estates, Inc.*, 581 U.S. 433, 439, 137 S. Ct. 1645, 198 L. Ed. 2d 64 (2017) (quotation omitted). Rather, "a plaintiff must demonstrate standing separately for each form of relief sought." *Friends of the Earth, Inc. v. Laidlaw Env. Servs. (TOC), Inc.*, 528 U.S. 167, 185, 120 S. Ct. 693, 145 L. Ed. 2d 610 (2000). So a plaintiff could, for example, have standing

to seek damages from the defendant but lack standing to seek an injunction. *See City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 103 S. Ct. 1660, 75 L. Ed. 2d 675 (1983).

These standing requirements apply equally to class actions. The individual named plaintiffs must therefore satisfy those requirements.[2] *See Warth v. Seldin*, 422 U.S. 490, 502, 95 S. Ct. 2197, 45 L. Ed. 2d 343 (1975). So, like any other plaintiffs, Bias, Cardenas, Holmes, and Shaw can each only proceed if they show an injury-in-fact caused by Elephant and redressable by the court for each form of relief sought. *Id.* This case turns primarily on whether their allegations establish the first requirement: injury-in-fact.[3]

All named plaintiffs—Bias, Cardenas, Holmes, and Shaw—assert that the breach of Elephant's network

2. In this appeal, we evaluate only the district court's finding that the named plaintiffs lacked Article III standing. As to the surviving damages claims, we note that "[e]very class member must have Article III standing in order to recover individual damages." *TransUnion*, 594 U.S. at 431.

3. Holmes alone pleaded an injury that the district court found was an injury-in-fact— an uptick in spam texts and calls to his phone after the data breach at Elephant. But as the district court accurately noted, "[t]he plaintiffs do not allege that the [compromised information] in this Data Breach included cell phone numbers." *Elephant Ins.*, 2023 U.S. Dist. LEXIS 110161, 2023 WL 4183380, at *6. This straightforwardly defeats Holmes's attempt to attribute his uptick in spam texts and calls to the data breach. Without much consternation, we affirm the district court's determination that "Holmes has failed to adequately allege traceability" for this injury. *Id.*

inflicted four injuries-in-fact: (1) the actual compromise of their personal information in the breach; (2) the risk of future misuse of their personal information by other malicious actors; (3) the risk of having their personal information taken again in the future in another hack of Elephant; and (4) the emotional distress and time spent monitoring their financial records to mitigate the likelihood of future harm. We address each alleged injury for each of the four plaintiffs to see if they are "concrete, particularized, and actual or imminent." *TransUnion*, 594 U.S. at 423.

A. Two Plaintiffs Suffered A Concrete Injury

Having one's information compromised by a data breach is a harm that is both particularized, by affecting each individual personally, and actual, by occurring in reality. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 339, 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016) . The difficulty is determining whether it is "concrete"—whether it is "real, and not abstract." *TransUnion*, 594 U.S. at 424 (quoting *Spokeo*, 578 U.S. at 340). Some harms are unquestionably concrete. "The most obvious are traditional *tangible* harms, such as physical harms and monetary harms." *Id.* at 425 (emphasis added). When a plaintiff alleges that he has been punched or had his wallet stolen, little more needs to be said.

Intangible harms are not so straightforward. To be sufficiently concrete, an intangible harm must bear "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Id.*

To determine whether an injury satisfies this standard, we must assess whether there is "a close historical or common-law analogue" to it, though the analogue need not be "an exact duplicate." *Id.* at 424.[4]

Notice what the Supreme Court tells us the relationship must be between: "harms." *Id.* at 425. Not elements. This concern with harm is apparent from the very first paragraph of *TransUnion*, which lists "physical," "monetary," and "reputational" harms without discussing the many distinct elements of the many distinct causes of action that protect against these types of harm. 594 U.S. at 417. For this reason, we have explained that under *TransUnion*, "our inquiry focuses on types of harms protected at common law, not the precise point at which those harms become actionable." *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 922 (4th Cir. 2022) (cleaned up) (quoting *Krakauer v. Dish Network, LLC*, 925 F.3d 643, 654 (4th Cir. 2019)).

This is not to say that the elements of a common-law cause of action are irrelevant. Defining the harm addressed by a cause of action can be difficult, especially when the harm is intangible. And when the harm addressed is not immediately obvious, the elements of the cause of action can shed light on the matter. Consider *TransUnion* itself. There, the Court assessed whether someone whose credit file contained a misleading "OFAC alert"— a warning stating that they had a name identical to one on a list of

4. *TransUnion* adds that "harms specified by the Constitution itself" can also be concrete without the need for a common-law analogue. 594 U.S. at 425. This case does not concern such harms.

potential terrorists and criminals—had suffered a harm sufficiently close to that inflicted by defamation. 594 U.S. at 432. The Court determined that the 1,853 plaintiffs whose misleading OFAC alerts were disseminated to a third party suffered a harm analogous to defamation and thus sufficient for concrete injury. *Id.* But for the 6,332 whose misleading OFAC alerts were not disseminated, the Court concluded otherwise. *Id.* at 434-35.

In explaining why the latter group lacked a concrete injury, the Court pointed to the elements of defamation, remarking that the element of "[p]ublication is 'essential to liability' in a suit for defamation." *Id.* at 434 (quoting Restatement of Torts § 577 cmt. a (Am. L. Inst. 1938)). Without publication of the OFAC alert in their credit files, the group of 6,332 plaintiffs could not analogize to defamation.[5] Critically, however, this was not because the Court required an element-to-element comparison with defamation. Instead, the Court found the lack of publication fatal to concrete injury because defamation's *harm* "was the loss of credit or fame, and not the insult"

5. In a footnote, the Court also considered the argument that the 6,332 plaintiffs whose OFAC alerts were not disseminated still suffered a concrete injury because the alert was seen "internally" by "employees within TransUnion." *TransUnion*, 594 U.S. at 434 n.6. The Court rejected this argument, explaining that "[m]any American courts did not traditionally recognize intra-company disclosures as actionable publications." *Id.* The Court added that "evidence that the document was actually read and not merely processed" was "lacking" from the plaintiffs. *Id.* It thus concluded that because "the plaintiffs' internal publication theory circumvent[ed] a fundamental requirement of an ordinary defamation claim," it could not support a finding of concrete injury. *Id.*

itself, and that harm could only occur when the defamatory information was known by others. *TransUnion*, 594 U.S. at 434 (quotation omitted). Publication did not matter because it was an element of defamation; it mattered because it helped define the harm of defamation.

But not all elements of a cause of action go to the harm addressed. Many common-law torts, for example, reserve liability for defendants who have acted with a certain culpable mental state. Take the tort of false imprisonment. To be liable for false imprisonment, a defendant must act "intending to confine" the plaintiff, at least when the imprisonment does not otherwise threaten bodily harm. Restatement (Second) of Torts § 35 & illus. 2 (Am. L. Inst. 1965). Yet a day trapped in a storage closet is a day trapped in a storage closet whether it is brought about intentionally or not; the tangible harm of the confinement is independent of the defendant's intentions. So a person imprisoned by accident will have standing to sue. The victim has suffered regardless of the defendant's liability. More generally, elements that pertain to the details of the defendant's action will often—though not always—be unrelated to the kind of harm felt by the victim.[6] At all times, the concreteness analysis must be focused on the

6. We do not deny the possibility that in some cases, the intentions of the defendant could help define the harm to the victim. But this will only occur when it is important that the defendant's intentions be known or apparent. What matters in those cases is not the defendant's mental state itself but the way the plaintiff perceives that mental state. For instance, knowing that someone has injured you on purpose may cause particular offense or instill fear of future harm.

harm addressed by the analogous cause of action, not on the cause of action's elements.[7]

1. Having one's driver's license number listed on the dark web bears a close relationship to a harm recognized at common law

Now to apply *TransUnion*'s harm-analogue test to this case. The plaintiffs here seek to analogize the harm from Elephant's data breach to the harm addressed by the tort of public disclosure of private information—a harm mentioned by name as a permissible common-law analogue.[8] *TransUnion*, 594 U.S. at 425. Public disclosure

---

7. This focus on harm over elements is shared by our sister circuits. *See, e.g., Barclift v. Keystone Credit Servs., LLC*, 93 F.4th 136, 145 (3d Cir. 2024) ("*TransUnion* speaks only of harms, not elements."); *Drazen v. Pinto*, 74 F.4th 1336, 1343 (11th Cir. 2023) (en banc) (requiring the presence of "element[s] essential to the harm" in assessing common-law analogues); *Nabozny v. Optio Sols. LLC*, 84 F.4th 731, 734 (7th Cir. 2023) (listing several examples of the types of harm that provide standing); *Shields v. Pro. Bureau of Collections of Md., Inc.*, 55 F.4th 823, 829 (10th Cir. 2022) (stating that the plaintiff "did not have to plead and prove the tort's elements to prevail" but had "to at least allege a similar harm").

8. Elephant argues that public disclosure of private information cannot serve as a *TransUnion* analogue because it "is not recognized under Virginia common law." Resp. Br. 7, 17. True, at least since 1977. *See WJLA-TV v. Levin*, 264 Va. 140, 564 S.E.2d 383, 394 n.5 (Va. 2002). But this matters not. *TransUnion* does not ask for an analogue recognized in the specific jurisdiction whose laws are being applied. It only asks for an analogue "traditionally recognized" in history or at common law in general. *TransUnion*, 594 U.S. at 425. Virginia's relatively recent actions in this area are irrelevant in

of private information is one of four "invasion of privacy" torts historically recognized at common law.[9] *See* William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 389 (1960). It requires that the defendant (1) disclose (2) to the public (3) true but private information that would be highly offensive to a reasonable person and (4) is otherwise of no legitimate concern to the public. *See* Restatement (Second) of Torts § 652D & Special Note & cmt. a; *Cape Publications, Inc. v. Hitchner*, 549 So. 2d 1374, 1377 (Fla. 1989); *Shulman v. Group W Productions, Inc.*, 18 Cal. 4th 200, 74 Cal. Rptr. 2d 843, 955 P.2d 469, 478 (Cal. 1998).

What harm is the public disclosure of private information tort aimed at? It is chiefly concerned with the dissemination of information regarding "[s]exual relations," "family quarrels," and "humiliating illnesses" to a large number of individuals. Restatement (Second) of Torts § 652D cmt. b. But the public-disclosure tort shields more information than just the inherently shameful. It extends to cover situations where publicity has been given to "income tax returns," suggesting that the private information need not be so sordid as to find a home on Page Six. *Id.* Nor is it limited to information that has been kept completely confidential. A woman who agrees to film her "caesarian operation . . . for exhibition to medical students for educational purposes" cedes much of her privacy for

---

light of the widespread recognition of the tort of public disclosure of private information.

9. The other three are intrusion upon seclusion, misappropriation of name or likeness, and false publicity. *See* Restatement (Second) of Torts § 652A.

a particular purpose, and yet she can still sue if the film of her operation is then shown "in a commercial theater." *Id.* § 652D illus. 11. So even information that is revealed in some contexts can remain private as to the public at large.

A closer look at the elements of the public disclosure of private information allows us to refine our understanding of its harm. While the tort covers a wide range of information, two of its elements—that the information be highly offensive to a reasonable person if shared, and that it not be of legitimate public concern—tell us that only sensitive personal information falls within the scope of the tort. Other pieces of nonsensitive personal information can be shared without inflicting actionable harm. So while an idiosyncratic recluse may be distressed by the publicization of his hair color or his favorite flavor of ice cream, the tort does not protect such anodyne facts. *See id.* § 652D cmt. c ("[A]nyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part.").

And the publicity element makes clear that even when sensitive personal information is at issue, actionable harm does not occur any time that information is shared without permission. The tort is only implicated when the sharing is so broad that it "reaches, or is sure to reach, the public." *Id.* § 652D cmt. a. Publicity is given to information "broadcast over the radio," or given "to a large audience," or published "in a newspaper or a magazine, even of small circulation," but not to statements made "to a small group of persons." *Id.* So while a confidante may breach her friend's trust by sharing her friend's intimate secret with

a handful of family members, the tort is unconcerned with such small-scale disclosures. Overall, the public disclosure of private information is aimed at the harm that occurs when sensitive personal information is released into the open.

Importantly, however, our question is not whether the harm inflicted by Elephant would be actionable under the public-disclosure tort. Rather, under *TransUnion*, the plaintiffs have standing so long as their harm is similar to the harm protected by a common-law cause of action. They need not an "exact duplicate" but an "analogue." *TransUnion*, 594 U.S. at 424. While the relationship between harms cannot be so "loose[]" as to serve as an "open-ended invitation for federal courts" to create new bases for standing divorced from history and tradition, the set of harms *analogous* to those actionable at common law is necessarily broader than the set of harms *actually* actionable at common law. *Id.* at 424-25.

TransUnion gives a specific clue about how far the analogous harms can extend by telling us that the harm in *Davis v. FEC*, 554 U.S. 724, 128 S. Ct. 2759, 171 L. Ed. 2d 737 (2008), is sufficiently close. *TransUnion*, 594 U.S. at 425. *Davis* is a campaign finance First Amendment case that involved a challenge to a federal law that required political candidates to report the total amount of expenditures they made in their own campaigns over a certain threshold. *Davis*, 554 U.S. at 729-32. The harm of disclosing the amount of such campaign expenditures thus must bear a close relationship to the harm "traditionally recognized" by the public-disclosure tort.

But the amount a candidate spends on his campaign—a bare dollar figure without detail—is not information that would be considered personally sensitive in a way that is actionable under the public-disclosure tort. It is merely information that, though dry and numerical, a candidate may justifiably wish to tightly control (because he wishes to avoid being seen as wealthy and out-of-touch by voters, for example). So though the public-disclosure tort may be limited to sensitive personal information, *TransUnion*'s invocation of *Davis* tells us that it furnishes standing by analogy for more.

Because the campaign expenditure amount in *Davis* was certain to be made publicly available by law, *see* 52 U.S.C. § 30104(a)(11)(B), *Davis* does not help us determine whether the public-disclosure tort's requirement of publicity is similarly broadened. We conclude the answer is no—publicity cannot be broadened under *TransUnion* to include disclosures that would be considered private at common law. Sensitive personal information and justifiably withheld information, like false statements and misleading statements, differ in degree. *See TransUnion*, 594 U.S. at 433. But public disclosure and private disclosure strike us as differing in kind. "Private disclosure is not just a less extreme form of public disclosure. Publicity causes a qualitatively different harm." *Hunstein v. Preferred Collection and Mgmt. Servs., Inc.*, 48 F.4th 1236, 1249 (11th Cir. 2022) (en banc); *see also* Restatement (Second) of Torts § 652D cmt. a (drawing a sharp "distinction . . . between private and public communication"). An announcement to a crowd is not simply a more efficient way of conducting a series of one-on-one conversations; it is a

different way of communicating altogether. So harms that analogize to the harm of the public disclosure of private information must still involve publicity.

Viewing this all together through the lens of *TransUnion*, we hold that the public disclosure of private information tort makes concrete the intangible harm suffered when information that the plaintiff would justifiably prefer to tightly control is released into the open. Though the information need not be embarrassing or salacious, the plaintiff must have good reason to keep it close to the vest. And though the information need not be broadcast to the whole world, it must be accessible to many.

With this understanding in mind, we can determine whether the plaintiffs have alleged facts that show they have suffered a concrete injury from the Elephant data breach. Our answer is that they have—but only for two of the named plaintiffs.

The complaint contains sufficient allegations to show why all four plaintiffs justifiably desire to keep their driver's license numbers confidential. The plaintiffs tell us that driver's license numbers are "critical to easily forging an identity" using a full profile of information that includes other "[u]nique and persistent identifiers." J.A. 53. The numbers can be used "alone or in combination with other information" to "[o]pen bank accounts" and "[a]pply for financial loans." J.A. 55. And they are often "the critical missing link for a fraudulent unemployment benefits application." J.A. 61. So it is no surprise that the plaintiffs wish to protect such information from being known by the

public at large, and certainly by the unsavory individuals that often trawl the dark web.

But Bias and Shaw do not provide any reason to think that their driver's license numbers are now generally accessible. We are told that the hackers possess their driver's license numbers, but they do not allege that the unnamed hackers are so numerous as to constitute the public on their own. Nor do they allege that the hackers have shared their driver's license numbers with anyone else. As far as we are told, their stolen information is currently accessible to only a few. So the harm felt by Bias and Shaw does not bear a close relationship to the harm addressed by the public-disclosure tort. If the hackers' private knowledge of their driver's license number inflicts a harm, it is a harm different in kind, not degree, from that addressed by the common-law tort. The two of them have not alleged a concrete injury.

The two other named plaintiffs—Cardenas and Holmes—are different. They allege that they found their driver's license numbers listed on the dark web and attribute the listings to the Elephant breach.[10] The dark

10. Strictly speaking, Cardenas only alleges that he found her information for sale on the dark web, which implies that his full driver's license number is only accessible with payment. But we do not see why this should make a difference. One classic example of publicity in public-disclosure tort cases is listing information in a newspaper. *See* Restatement (Second) of Torts § 652D cmt. a ("[A]ny publication in a newspaper or a magazine, even of small circulation . . . is sufficient to give publicity."). Yet many newspapers are only accessible with payment too. We see no reason to treat the internet

web, an anonymous online network for unregulated content and markets, is not a traditional method of communicating information like a newspaper or radio broadcast. But, not dissimilar to the internet more generally, it is a forum accessible to all—or at least to those with some degree of proficiency with computers. Information listed on it thus either "reaches, or is sure to reach, the public," or is close to doing so. Restatement (Second) of Torts § 652D cmt. a. So Cardenas and Holmes have alleged facts showing that information they justifiably prefer to tightly control has been released into the open. Under *TransUnion*, that is sufficient to show a concrete injury in the eyes of Article III.[11]

2. Elephant's counterarguments are unavailing

Elephant attacks the *TransUnion* analogy between the plaintiffs' alleged harm and the public disclosure of private information tort in two ways. Neither succeeds.

First, Elephant argues that the plaintiffs' theory of concrete injury should fail because they cannot satisfy one element required for liability under the public-

---

differently. Paywalled or not, information listed on the internet is ordinarily accessible to many.

11. In so concluding, we join the First, Second, and Third Circuits, which have recently issued opinions finding concrete injury under *TransUnion* in similar situations. *See Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365 (1st Cir. 2023); *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276 (2d Cir. 2023); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d. Cir. 2022).

disclosure tort: that Elephant made a disclosure.[12] That is, in Elephant's view, an analogy only exists if Elephant had exposed their driver's license numbers through some affirmative action. *See Disclose, Black's Law Dictionary* (6th ed. 1990) ("To bring into view by uncovering; to expose; to make known."). And Elephant asserts that it took no such action—that it and the plaintiffs alike were passive victims of a hack.

But this misunderstands *TransUnion* for reasons already given. Recall that *TransUnion* only seeks a "close relationship" between *harms*, not elements. 594 U.S. at 425. So the only elements that matter are the ones that define the harm of the analogous cause of action. A defendant's disclosure, though also *an* element of the public disclosure of private information tort, is not a *harm-defining* element—it goes to the defendant's liability, not to what is felt by the plaintiff. Someone whose driver's license number is made accessible to many is harmed by that loss of control over their private information, even if the situation was brought about through no fault or action of the defendant.[13] Though the defendant cannot be held

12. Though case law tends to use the word "disclosure," the Restatement eschews the term, instead speaking in terms of "giving publicity." Restatement (Second) of Torts § 652D. This terminological difference does not change our understanding of the tort.

13. Plaintiffs argue that even if active disclosure were required under *TransUnion*'s analogue test, it was satisfied here because Elephant intentionally designed its online quoting platform with an auto-populate feature. Since we hold that the element of disclosure is immaterial to our standing analysis, we have no occasion to address this argument.

liable under the public-disclosure tort without disclosure, there is still a concrete injury.[14]

Second, Elephant points out that a divided panel of the Seventh Circuit has held, in a case nearly identical to this one, that a driver's license number is not sufficiently close to the kind of sensitive information protected by the public disclosure of private information tort. In that case, *Baysal v. Midvale Indemnity Co.*, plaintiffs brought a putative class action suit against an insurer after the plaintiffs' driver's license numbers were compromised in a data breach using the insurer's auto-populated quoting platform. 78 F.4th 976, 977 (7th Cir. 2023). The Seventh Circuit affirmed the dismissal of the case for lack of standing under *TransUnion*, reasoning that only "potentially embarrassing or intimate details" are shielded by the public disclosure of private information, and "[a] license number is not viewed as embarrassing . . . or private . . . but as neutral." *Id.* at 979.

As our discussion should make clear, we see things differently. Undoubtedly, a driver's license number is unlike the details of an affair or a medical condition. People do not consider their driver's licenses embarrassing and hand them to bartenders and waiters and police officers without hesitation. But we know that the public-disclosure tort protects some types of information that we would not

14. To put a fine point on it: Elephant's argument elides the distinction between what is needed for standing under the common-law analog and what is needed to prove liability under the common-law analog. Allegations that would fall short of proving liability can nevertheless establish standing. These are separate inquiries.

strictly consider embarrassing. *See* Restatement (Second) of Torts § 652D cmt. b (listing "income tax returns"). And we also know that *TransUnion* requires harms that are analogues, not duplicates, which further broadens the set of information whose dissemination may inflict a concrete injury. So we cannot accept that a concrete injury exists only if the information publicized is embarrassing.

Indeed, the Seventh Circuit appeared to recognize as much when it implied in the very same opinion that publicizing social security numbers *would* be concrete injury. *Baysal*, 78 F.4th at 977, 979. But social security numbers are also "not viewed as embarrassing . . . or private . . . but as neutral," and "most adults have these numbers, which are neither good nor bad." *Id.* at 979. While driver's license numbers may be *less* private than social security numbers,[15] such a difference would be a difference in degree, not a difference in kind—and *TransUnion* only requires an analogy by kind. *See TransUnion*, 594 U.S. at 424; *see also Garey*, 35 F.4th at 922 (explaining that the *TransUnion* inquiry compares "types of harms").[16]

---

15. The plaintiffs assert that this may not even be true, telling us that the value of a driver's license number is the same as a social security number on the dark web. If the privacy information is correlated with its value to malicious actors, the two pieces of information would appear to be equally private—or at least equally capable of dealing damage when misused by the wrong party.

16. We caution that while we disagree with the Seventh Circuit on the bottom line, we agree that there is a "need to be precise when thinking about invasion of privacy" torts and how they furnish standing. *Baysal*, 78 F.4th at 980. The harm inflicted by each of the four invasion-of-privacy torts is not the same; each

If publicizing social security numbers would inflict a kind of concrete injury, we see no reason why driver's license numbers would be different.

Notably, Congress appears to agree with us. *TransUnion* reminds us that "[i]n determining whether a harm is sufficiently concrete to qualify as injury in fact . . . Congress's views may be 'instructive.'" 594 U.S. at 425 (quoting *Spokeo*, 578 U.S. at 341). And here, Congress has enacted the Driver's Privacy Protection Act, which provides a cause of action against "a person who knowingly obtains, *discloses*, or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter," which includes driver's license numbers. 18 U.S.C. § 2724 (emphasis added). To be sure, "we cannot treat an injury as 'concrete' . . . based only on Congress's say-so." *Id.* at 426 (quotation omitted). But "our assessment of concreteness must look to '*both* history *and* the judgment of Congress.'" *Baysal*, 78 F.4th at 981 (Ripple, J., dissenting) (emphasis added) (quoting *Spokeo*, 578 U.S. at 340). Respect for "Congress' role in identifying and elevating intangible harms" thus requires us to give weight to the harms it chooses to protect by statute. *Spokeo*, 578 U.S. at 341. Though driver's license numbers may not be the most sensitive personal information people possess, they are, in Congress's view, among the "personal information" worth protecting. § 2725(3). That favors finding the injury here concrete.

---

must be taken on its own terms. What is true for public disclosure of private information, for example, may not be true for intrusion upon seclusion. *See, e.g.*, Prosser, *supra*, at 389-90, 398 (tracing the roots of public disclosure of private information to defamation but the roots of intrusion upon seclusion to trespass).

In sum, Cardenas and Holmes have had their driver's license numbers listed on the dark web against their justifiable wishes. Under *TransUnion*, they have suffered a concrete injury. And because that injury has already come to pass, it gives them standing to seek damages. *See Lyons*, 461 U.S. at 105. On this specific basis for injury-in-fact, only for retrospective relief like damages, and only for Cardenas and Holmes, we reverse the district court's decision.

B. Plaintiffs' Other Alleged Injuries Do Not Support Standing

The plaintiffs' other standing theories do not fare so well. The risk that their driver's license numbers may be misused in the future fails to furnish standing because they have not alleged facts showing that any particular misuse is imminent. The risk that another data breach may befall Elephant in the future fails for the same reason. And the lack of imminent injury prevents the plaintiffs from bootstrapping their way into standing for damages solely by expending time or alleging emotional distress.

1. Plaintiffs have not shown any further future misuse is imminent

The plaintiffs' second asserted injury-in-fact is the risk that someone may misuse their driver's license numbers in the future. In the plaintiffs' words, they are at an "increased risk of identity theft." J.A. 71. But the plaintiffs use the phrase "identity theft" more broadly than is conventional. They suggest that the posting of information on the dark web is itself "identity theft."

See, e.g., J.A. 76 (Plaintiff Holmes's "information was on the dark web, proof that his identity has been stolen."). So we consider the plaintiffs to have actually alleged two distinct risks. Bias and Shaw allege that they are at risk of having their information publicized. And Cardenas and Holmes, who have already had their information publicized on the dark web, allege that they are at risk of having their identity further misused as part of a fraudulent impersonation attempt.[17]

The two alleged future harms are both concrete and particularized.[18] So they may furnish standing to seek

17. This second risk to Cardenas and Holmes is what we understand the conventional definition of "identity theft" to be. It requires the use of personal information in a fraudulent impersonation attempt for personal gain. *See McMorris v. Carlos Lopez & Assocs.*, 995 F.3d 295, 302 (2d Cir. 2021) (distinguishing posting personal information on the dark web from "actual or attempted identity theft"); *see also Identity Theft*, Department of Justice Criminal Division (Aug. 11, 2023) ("Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains *and uses another person's personal data in some way that involves fraud or deception*, typically for economic gain." (emphasis added)). To avoid confusion between this conventional definition and the plaintiffs' broader definition, we eschew the use of the phrase "identity theft" in this section.

18. The first injury, of having one's information posted on the dark web, is concrete for reasons given above. The second injury, of having one's identity fraudulently misrepresented, is concrete because it either inflicts a tangible injury, *see, e.g., Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (eleven point decrease in credit score from a fraudulent credit card application), or will inflict an intangible injury that is on all fours with the common-law tort of appropriation of another's name or likeness, *see* Restatement (Second) of Torts § 652C.

prospective declaratory and injunctive relief if the future harm is "imminent." *Lujan*, 504 U.S. at 564. A future harm is not imminent just because there is an "objectively reasonable likelihood" that it will someday come to pass. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013). Instead, "the plaintiffs must show a substantial risk that" it will happen "in the near future." *Murthy v. Missouri*, 603 U.S. 43, 58, 144 S. Ct. 1972, 219 L. Ed. 2d 604 (2024).[19] While imminence "is concededly a somewhat elastic concept," *Lujan*, 504 U.S. at 564 n.2, we conclude that neither alleged future harm establishes a substantial risk of future misuse of their driver's license numbers.

First, Bias and Shaw. Their assertion of imminence runs headlong into *TransUnion*. The 6,332 plaintiffs in *TransUnion* who did not have their inaccurate credit reports disseminated, in addition to alleging that they suffered an actual injury, also alleged that they faced an imminent injury because "TransUnion could have divulged their misleading credit information to a third

19. The Supreme Court has used multiple phrases to express this concept. *See, e.g., Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158, 134 S. Ct. 2334, 189 L. Ed. 2d 246 (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." (quotation omitted)). Until recently, it was unclear whether "certainly impending" and "substantial risk" expressed the same or different standards. *See Clapper*, 568 U.S. at 414 n.5 ("But to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement . . ."). But recently, the Court has treated the two as one, using "substantial risk" as the preferred language. *See, e.g., Murthy*, 603 U.S. at 58. We follow the Court's more recent gloss on the *Clapper* standard.

party at any moment." *TransUnion*, 594 U.S. at 438. But the Court dismissed this "risk of dissemination to third parties" as "too speculative" to establish an imminent injury because the plaintiffs had given no reason to think it would occur. *Id.* The fact that other members of the class already had their information disseminated was not enough to establish imminence.

Bias and Shaw are in a position that is materially indistinguishable from the 6,332 plaintiffs in *TransUnion*. The hackers who breached Elephant could presumably post their driver's license numbers to the dark web "at any moment." But they have given us no reason to think that this will occur. Their strongest piece of evidence is that the hackers have already posted Cardenas and Holmes's information to the dark web, suggesting that more information from the breach may follow. But that fact did not suffice for imminence in *TransUnion* itself. We see no reason it would be different here.

Cardenas and Holmes are in a different position. Because they have already had their driver's license numbers listed on the dark web, the future misuse they worry about will come from a malicious actor's fraudulent impersonation attempt. Bias and Shaw, of course, cannot show that fraudulent impersonation is imminent because they falter at an earlier step. Though Cardenas and Holmes have a head start, they arrive at the same place.

Specifically, Cardenas and Holmes's position is foreclosed by the principle we stated in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017). In *Beck*, an employee's laptop

and four boxes of medical reports were stolen from a veterans' hospital. *Id.* at 267-68. Patients of the hospital sued the hospital for the data breach, alleging violations of the Privacy Act of 1974 and the Administrative Procedure Act. *Id.* at 266. But the district court dismissed their suit for lack of standing, and this Court affirmed. *Id.* at 277-78. In doing so, we set out a numerical bar for imminence in the context of data breaches: "Even if we credit the Plaintiffs' allegation that 33% of those affected by [the data breach] will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm." *Id.* at 275-76. So *Beck* tells us that the probability needed for "substantial risk" is at least 33%—and presumably a good bit higher.[20]

Cardenas and Holmes do not clear that bar. They do not allege that their driver's license numbers have been

---

20. We are bound here to apply *Beck*'s statistical floor. *See Payne v. Taslimi*, 998 F.3d 648, 654 (4th Cir. 2021). But one might understand *Beck* to not extend beyond the context of data breaches and other similar informational injuries. *See Beck*, 848 F.3d at 276; *cf. Sommerville v. Union Carbide Corp.*, 149 F.4th 408, 421 (4th Cir. 2025) (finding *Beck* inapposite because plaintiff's "injury is a present physical one" that "exists *already*"). What qualifies as a "substantial risk" *might* vary from injury to injury—in other words, "substantial risk" might encompass expected value, not just pure probability. *See, e.g., Mountain States Legal Found. v. Glickman*, 92 F.3d 1228, 1234, 320 U.S. App. D.C. 87 (D.C. Cir. 1996) ("The more drastic the injury that government action makes more likely, the lesser the increment in probability necessary to establish standing."). While we note the possibility, we take no position on *Beck*'s reach or on whether this distinction might reflect modern standing doctrine.

misused by the hackers to date. So any future harm, given that the hackers have posted their information on the dark web, would presumably come from the intervening actions of independent malicious actors who might buy or otherwise obtain their compromised numbers. *Clapper*, 568 U.S. at 413. But they have not alleged facts that show that those intervening "independent decisionmakers" "will likely react in predictable ways" that will ultimately result in fraudulent impersonation. *Murthy*, 603 U.S. at 58 (quoting *Dep't of Com. v. New York*, 588 U.S. 752, 768, 139 S. Ct. 2551, 204 L. Ed. 2d 978 (2019)).

Instead, the plaintiffs offer only a "speculative chain of possibilities." *Id.* at 70 (quoting *Clapper*, 568 U.S. at 414). To start, the plaintiffs do not allege anything that suggests that their specific driver's license numbers will be acquired by identity thieves off the dark web.[21] To be sure, hackers list personal information on the dark web in the hope that someone will buy it. But no particular piece of personal information is guaranteed to be seen or sold, just as no particular item on Craigslist or eBay is guaranteed to be seen or sold. Without more, it is unrealistic to assume that identity thieves will imminently acquire the driver's license number of any given plaintiff.

There is another link in the speculative chain. As the plaintiffs themselves explain, one single piece of personal information is not enough for fraudulent impersonation;

21. Holmes alleges that his driver's license number was "found" on the dark web but does not clarify if it was found in its entirety for free or whether it was simply for sale. Cardenas expressly alleges that his number was for sale.

impersonators must usually "aggregate information taken from data breaches on users to build profiles on individuals" before attempting to impersonate someone. J.A. 53. The district court recognized as much. *See Elephant Ins.*, 2023 U.S. Dist. LEXIS 110161, 2023 WL 4183380, at *4 ("The driver's license number's real value lies in being pieced together with other [personal information] to create a full profile."). So even if Cardenas or Holmes's specific driver's license number was acquired, that enables fraudulent impersonation only if the impersonators also have enough information from other sources to build a profile.

And there is yet another link. Driver's license numbers do not stay valid for all eternity. "[L]icense numbers change over time as people move to different states or licenses are renewed." *Baysal*, 78 F.4th at 979.[22] Though perhaps harder to cancel than a credit card, driver's license numbers can still "be rendered useless to cybercriminals" more easily than many other forms of information. *McMorris*, 995 F.3d at 302. Driver's license numbers are thus part of, or close to, the category of

22. *Baysal* declined to find concrete injury under *TransUnion* on the grounds that driver's license numbers were insufficiently sensitive. As explained above, we believe that reasoning to be mistaken. So long as the plaintiffs justifiably seek to tightly control the set of people who know the information, the *degree* of sensitivity of the information does not help gauge whether its disclosure would work the *kind* of harm addressed by the public disclosure of private information tort. But the degree of sensitivity, including the ease of replacing the information, is perfectly at home in assessing whether the risk of future fraudulent impersonation is imminent—a wholly separate inquiry from concreteness. Different aspects of standing look to different facts.

"less sensitive data" that "does not pose the same risk of future identity theft or fraud to plaintiffs if exposed." *Id.* For many plaintiffs, then, "as the breach[] fade[s] further into the past," the risk they will be impersonated "become[s] more and more speculative." *Beck*, 848 F.3d at 275 (quotation omitted).

All this means that fraudulent impersonation will befall Cardenas and Holmes only if *other* intervening malicious actors acquire their driver's license numbers from the dark web *and* also acquire other pieces of their personal information *and* do so before their driver's license numbers change. And under our precedent, the plaintiffs cannot just assert that all this *might* happen; they must allege facts allowing us to conclude that for some particular plaintiff, the combined probability of that speculative chain materializing surpasses at least 33%. *See Beck*, 848 F.3d at 276-77. They have not done so. So they "fall[] far short of establishing a 'substantial risk' of harm." *Id.* at 276. Accordingly, neither Bias nor Shaw nor Cardenas nor Holmes have shown that they are at risk of an imminent injury.

We recognize that our sister circuits have found imminent injury to plaintiffs in similar circumstances to Cardenas and Holmes. *See, e.g., Bohnak*, 79 F.4th at 289 (finding imminent injury when names and SSNs were compromised in a hack); *Webb*, 72 F.4th at 375-76 (finding imminent injury from future use of detailed pharmacy records compromised in a hack); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29, 431 U.S. App. D.C. 273 (D.C. Cir.

2017) (finding imminent injury from future use of names and health insurance numbers compromised in a hack); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693-94 (7th Cir. 2015) (finding imminent injury from future use of credit card numbers compromised in a hack). And several cases identify the targeted nature of an attack and the subsequent listing of the information on the dark web—both present here—as factors weighing in favor of standing. *See, e.g., McMorris*, 995 F.3d at 301; *Clemens*, 48 F.4th at 157; *Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889-90 (11th Cir. 2023).

But our sister circuits have not explained how a data breach presents a substantial risk that any one piece of personal information will be misused in the future, even when the plundered information is listed on the dark web. None run through the chain of independent events and third-party choices that would have to coalesce for future fraudulent impersonation to befall any particular plaintiff. Rather, many cases appear to implicitly require only a reasonable probability of future harm—a looser notion of imminence urged by the dissent in *Clapper* but rejected by the majority. *See Clapper*, 568 U.S. at 432-33, 441 (Breyer, J., dissenting). Following "the common-sense notion that a threatened event can be reasonably likely to occur but still be insufficiently imminent to constitute an injury-in-fact," *Beck*, 848 F.3d at 276 (cleaned up), this Court has drawn a tighter boundary when it comes to future harms. The plaintiffs may have alleged enough to show that the risk of future misuse is an imminent injury before other courts. But they have not done so before this one.

2. Plaintiffs have not shown another breach will occur at Elephant

Next, the plaintiffs assert another future harm: a second data breach at Elephant that might compromise more of their information in the same way. To redress this alleged injury, they ask us to declare that Elephant's security is unlawfully shoddy and enjoin Elephant to fix it by, among other things, hiring security auditors, deleting unused customer data, and conducting routine internal security training sessions. We have already determined that such a data breach would be a concrete injury if the compromised information was then made accessible to many, as by sharing the information on the dark web. And it would be particularized to any person whose information was compromised. So the question, again, is whether the risk of this future injury is imminent enough to itself be an injury-in-fact.

The answer, again, is no. On this front, the plaintiffs run headlong into the Supreme Court's decision in *City of Los Angeles v. Lyons*. In *Lyons*, police placed Adolph Lyons into a chokehold at a traffic stop. 461 U.S. at 97. Along with retrospective damages for the incident, Lyons sought a prospective injunction ordering the Los Angeles Police Department to revise its use-of-force policies to bar chokeholds outside of situations requiring deadly force. *Id.* at 98. Despite the fact that Lyons had been previously placed in a chokehold, the Court held that Lyons had no standing to seek such relief. *Id.* at 109. Even though "there [would] be certain instances in which strangleholds

[would] be illegally applied" by the Los Angeles Police Department to denizens of the city, the certainty of unconstitutional action in the aggregate did not mean that "Lyons himself [would] again be involved in one of those unfortunate instances." *Id.* at 108. And without alleging anything to support that he, specifically, had a substantial risk of suffering future harm, Lyons could not establish standing for prospective relief. *Id.* at 105-06, 111. Lyons was "no more entitled to an injunction than any other citizen." *Id.* at 111.

Lyons maps neatly onto this case. The plaintiffs here make only general allegations that "it is axiomatic" that a database hacked once "due to inadequate security measures" is thereby at risk of imminent additional breaches "unless those security measures are improved." Op. Br. at 48. But they give us no reason to think this is true—or that hackers would target Elephant again, specifically, as opposed to other companies that have recently suffered data breaches. Nor do they give any reason to think another data breach at Elephant would compromise their information, specifically, as opposed to information belonging to others. All the plaintiffs can show is that they are on the same footing as anyone else whose information was compromised in a data breach in the past few years. That "falls far short of the allegations that would be necessary to establish a case or controversy." *Lyons, 461 U.S.* at 105. If the possibility of being subject to another chokehold was insufficiently imminent in *Lyons*, the possibility of being subject to another data breach is insufficiently imminent here.

3. Without a separate imminent injury, Bias and Shaw cannot recover damages for time spent or emotional distress felt

Finally, the plaintiffs assert that they have suffered an injury-in-fact sufficient for damages by spending time monitoring their financials and by feeling emotional distress in response to the data breach at Elephant.[23] Because Cardenas and Holmes have already shown an injury-in-fact sufficient for damages, this assertion is inapplicable to them; there is no such thing as double standing for one form of relief.[24] But this assertion matters greatly for Bias and Shaw, who have no other basis to recover damages.

Neither the Supreme Court nor the courts of appeals have settled whether either time spent or emotional

---

23. Although the plaintiffs' amended complaint repeatedly refers to the "out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft," J.A. 80, the complaint has no allegations that the plaintiffs spent money after learning of the breach. The most the plaintiffs allege is that they spent time. So we take the "out-of-pocket costs" to refer solely to time, as the district court did. *See Elephant Ins.*, 2023 U.S. Dist. LEXIS 110161, 2023 WL 4183380, at *5.

24. To be clear, mitigation time and emotional distress are irrelevant to Cardenas and Holmes *for standing*. They may be relevant down the line when calculating the amount of their compensatory damages. *See* Restatement (Second) of Torts § 652H (recognizing both "mental distress" and "special damage" as recoverable for an invasion of privacy tort); *FAA v. Cooper*, 566 U.S. 284, 295, 132 S. Ct. 1441, 182 L. Ed. 2d 497 (2012) (explaining that "special damages" are "actual pecuniary loss[es]" that are incurred from an invasion of privacy (quotation omitted)).

distress felt are concrete injuries bearing a close relationship to harms recognized at common law. *See TransUnion*, 594 U.S. at 436 n.7 ("We take no position on whether or how such an emotional or psychological harm could suffice for Article III purposes."); *Perez v. McCreary, Veselka, Bragg & Allen, P.C.*, 45 F.4th 816, 825 (5th Cir. 2022) ("[W]e are not aware of any tort that makes a person liable for wasting another's time . . . [but] we do not conclusively decide whether such injuries are closely related to traditional harms."). We need not settle these questions today. Assuming without deciding that both are sufficiently concrete, we hold that Bias and Shaw cannot furnish standing f*or damages* solely through expenditures of time and allegations of emotional distress.

To start, we know that plaintiffs "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not [imminent]." *Clapper*, 568 U.S. at 402. When the future harm is imminent, a plaintiff may have standing to sue based on monetary costs that "remain[] fairly traceable to" the threat. *FEC v. Ted Cruz for Senate*, 596 U.S. 289, 297, 142 S. Ct. 1638, 212 L. Ed. 2d 654 (2022). But when the future harm is merely speculative, a plaintiff cannot backdoor standing "simply by making an expenditure based on a nonparanoid fear." *Clapper*, 568 U.S. at 416. "If the law were otherwise, an enterprising plaintiff" could conjure standing from nothing, "improperly water[ing] down the fundamental requirements of Article III." *Id.*[25]

25. It is unclear whether this rule against freestanding mitigation costs goes to the injury-in-fact or the traceability prongs of standing. It may be that expenditures made in response to a speculative event "are not fairly traceable to" that event. *Clapper,*

We see no reason to treat mitigation time differently than mitigation costs. The worry with finding standing based on mitigation costs alone is that anyone can pay to mitigate anything, however unlikely. The same worry exists for time. The only difference is that rather than spend a dollar, plaintiffs could spend a minute. Just as plaintiffs cannot circumvent their burden to show substantial risk by tacking on a claim for mitigation costs, we think plaintiffs cannot circumvent their burden by tacking on a claim for mitigation time. Allowing the latter would defeat the purpose of *Clapper*'s rule against the former and place the existence of an Article III case or controversy entirely in the hands of every plaintiff. We decline this invitation to gut the law of standing.

So too with emotional distress. Under *Clapper*, a plaintiff cannot "manufacture standing" by resort to a theory that would permit standing in every case. 568 U.S. at 402. And although emotional distress is distinct from mitigation expenditures, it poses much the same problem. Though a plaintiff does not choose to suffer emotional distress the way he might choose to spend time or money,

---

568 U.S. at 416; *see also id.* at 417 ("[R]espondents' present injuries are not fairly traceable to [the challenged statute]."). It may also be that mitigation cost is a unique kind of injury such that a plaintiff cannot plead it alone—that mitigation costs must connect with a second injury to be an injury-in-fact. *See, e.g., Hutton*, 892 F.3d at 622 ("[C]osts for mitigating measures to safeguard against future identity theft may not constitute an injury-in-fact when that injury is speculative."); *Remijas*, 794 F.3d at 694 ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent."). Either way, the result is the same—mitigation costs cannot furnish standing on their own.

a plaintiff can freely allege emotional distress in every case with little fear of disproof. For this reason, tort law has long aimed a skeptical eye at freestanding emotional distress claims. "Because of the fear of fictitious or trivial claims, distrust of the proof offered, and the difficulty of setting up any satisfactory boundaries to liability, the law has been slow to afford independent protection to . . . emotional distress standing alone." Restatement (Second) of Torts § 46 cmt. b. Instead, the law has traditionally only recognized "recovery for emotional distress as an additional, or 'parasitic' element of damages" that must be attached to a separate injury. *Id.* § 47 cmt. b. The same protective measure applies in the standing context.

Accordingly, we hold that *if* time spent and emotional distress felt are concrete injuries, they may serve as the sole basis for standing to recover damages only when incurred in response to a separate imminent harm. They do not suffice for standing on their own. For reasons explained above, Bias and Shaw have failed to allege any imminent harm. So they lack standing to recover damages for any time spent or emotional distress felt too.

* * *

Bias, Cardenas, Holmes, and Shaw sued Elephant after their driver's license numbers were compromised in a breach of Elephant's network. Cardenas and Holmes had their driver's license numbers then posted on the dark web. The publicity given to their driver's license numbers inflicted a concrete harm sufficient to establish an actual injury-in-fact. Accordingly, the two of them—along with

anyone in their class, if their class is certified—can seek damages for that injury. But they cannot recover any other form of relief. And Bias and Shaw cannot recover at all. The requirements of Article III standing prohibit plaintiffs from receiving redress for speculative future injuries or for injuries incurred only in response to those speculative injuries. Accordingly, the judgment is

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED.

APPENDIX B — OPINION OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, RICHMOND DIVISION, FILED JUNE 26, 2023

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

Civil Action No. 3:22cv487

CHRISTOPHER HOLMES *et al.*, ON BEHALF OF THEMSELVES AND ALL SIMILARLY SITUATED PERSONS,

Plaintiffs,

v.

ELEPHANT INSURANCE COMPANY, *et al.*,

Defendants.

OPINION

This matter comes before the Court on a motion to dismiss filed by the defendants, Elephant Insurance Company, Elephant Insurance Services, LLC, and Platinum General Agency (collectively, "Elephant"). The plaintiffs[1] allege that Elephant did not adequately protect

1. The Consolidated Complaint names Christopher Holmes, Trinity Bias, Jaime Cardenas, and Robert Shaw as plaintiffs. It also indicates that these plaintiffs represent a class of similarly situated individuals that the plaintiffs will move to certify as a class if this case

their personal information ("PI") and that, in a data breach, malicious actors viewed and copied their PI. The plaintiffs bring a consolidated class action suit, asserting various claims arising from this data breach. Because the compromise of data, without more, does not constitute an injury-in-fact, the Court will grant Elephant's motion and dismiss the complaint because the plaintiffs lack standing.

I. FACTS ALLEGED IN THE CONSOLIDATED COMPLAINT

On May 6, 2022, Elephant announced to the public that they had detected unusual activity on their network (the "Data Breach"), and that "sensitive information" had been viewed or copied. (ECF No. 18 ¶ 7.) This information included "name, driver's license number, and date of birth." (*Id.* (quoting an Elephant News Release).) Elephant notified the plaintiffs that their information had been viewed by unauthorized actors. Elephant told the plaintiffs that Elephant had their personal information ("PI") because the plaintiffs "are . . . current or previous Elephant Insurance customer[s] or [Elephant] received [their] information as part of providing a quote for auto or other insurance coverage." (*Id.* ¶ 26 (quoting Elephant's "Notice of Data Incident" letter).)

Elephant's online quote tool auto-populated personal information after a user completed certain fields. Unauthorized actors took advantage of the auto-populate

---

proceeds to discovery. Throughout this Opinion, "plaintiffs" shall connote the four named plaintiffs and the potential class members.

feature to prompt Elephant to disclose the plaintiffs' PI. The four named plaintiffs include: (1) a previous Elephant customer (Robert Shaw); (2) a consumer who requested a quote for auto insurance (Jaime Cardenas); (3) an individual who does not remember if she requested a quote for auto insurance (Trinity Bias); and (4) an individual who asserts he never requested a quote for auto insurance (Christopher Holmes).

The plaintiffs assert eight claims against Elephant: violations of the Drivers' Privacy Protection Act (Count One); negligence (Count Two); negligence *per se* (Count Three); unjust enrichment (Count Four); violation of the Texas Consumer Protection Act (Count Five); violation of the Illinois Consumer Fraud Act (Count Six); violation of the Illinois Deceptive Trade Practices Act (Count Seven); and declaratory and injunctive relief (Count Eight). Elephant has moved to dismiss the complaint for lack of standing pursuant to Federal Rule of Civil Procedure 12(b)(1) and for failure to state a claim upon which relief may be granted pursuant to Federal Rule of Civil Procedure 12(b)(6).

II. RELEVANT LAW

A motion under Rule 12(b)(1) tests the Court's subject matter jurisdiction. As the party asserting jurisdiction, the plaintiff bears the burden of proving proper subject matter jurisdiction. *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). "[W]hen a defendant asserts that the complaint fails to allege sufficient facts to support subject matter jurisdiction, the trial court must apply a standard

patterned on Rule 12(b)(6) and assume the truthfulness of the facts alleged." *Kerns v. United States*, 585 F.3d 187, 193 (4th Cir. 2009).[2]

"In a class action, [courts] analyze standing based on the allegations of personal injury made by the named plaintiffs." *Beck v. McDonald*, 848 F.3d 262, 269 (4th Cir. 2017). As the party invoking federal jurisdiction, the plaintiffs bear the burden of establishing each element of standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice," and courts "accept as true [the plaintiffs'] allegations for which there is sufficient 'factual matter' to render them 'plausible on [their] face.'" *Beck*, 848 F.3d at 270 (first quoting *Lujan*, 504 U.S. at 561, then quoting *Ashcroft v. Iqbal*, 556 U.S.

2. A Rule 12(b)(6) motion gauges the sufficiency of a complaint without resolving any factual discrepancies or testing the merits of the claims. *Republican Party of N.C. v. Martin*, 980 F.2d 943, 952 (4th Cir. 1992). In considering the motion, a court must accept all allegations in the complaint as true and must draw all reasonable inferences in favor of the plaintiff. *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 253 (4th Cir. 2009) (citing *Edwards v. City of Goldsboro*, 178 F.3d 231, 244 (4th Cir. 1999)). The principle that a court must accept all allegations as true, however, does not apply to legal conclusions. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009). To survive a Rule 12(b)(6) motion to dismiss, a complaint must state facts that, when accepted as true, state a claim to relief that is plausible on its face. *Id.* "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007)).

662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009) (second alteration in the original)). Courts "do not, however, apply the same presumption of truth to 'conclusory statements' and 'legal conclusions.'" *Id.* (quoting *Bell Atl. Corp.*, 550 U.S. at 555-56).

"[T]he irreducible constitutional minimum of standing contains three elements." *Lujan*, 504 U.S. at 560. First, the plaintiff must have suffered "an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) actual or imminent, not conjectural or hypothetical." *Id.* (internal quotations omitted). "Second, there must be a causal connection between the injury and the conduct complained of." *Id.* "Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id.* at 561 (internal quotations omitted).

Statutory causes of action require an injury-in-fact. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341, 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016) ("Article III standing requires a concrete injury even in the context of a statutory violation."). "[P]laintiffs proceeding under a statutory cause of action can establish a cognizable injury by 'identif[ying] a close historical or common-law analogue for their asserted injury' for which courts have 'traditionally' provided a remedy." *Garey v. Farrin*, 35 F.4th 917, 921 (4th Cir. 2022) (quoting *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204, 210 L. Ed. 2d 568 (2021) (alteration in original)). "[U]nder Article III, an injury in law is not an injury in fact." *TransUnion LLC*, 141 S. Ct. at 2205.

First, an injury-in-fact, "the first and foremost of standing's three elements," may include threatened injuries, but "not all threatened injuries constitute an injury-in-fact." *Spokeo, Inc.*, 578 U.S. at 338 (internal quotation omitted); *Beck*, 848 F.3d at 271. "Allegations of possible future injury do not satisfy the requirements of Art[icle] III. A threatened injury must be 'certainly impending' to constitute injury in fact." *Whitmore v. Arkansas*, 495 U.S. 149, 158, 110 S. Ct. 1717, 109 L. Ed. 2d 135 (1990) (quoting *Babbitt v. Farm Workers*, 442 U.S. 289, 298, 99 S. Ct. 2301, 60 L. Ed. 2d 895 (1979)).

The "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018). The Fourth Circuit has consistently "held that being subjected to a data breach isn't in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft." *O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023). "[T]he mere theft of . . . items" containing personal information "cannot confer standing" because the threatened injury is too speculative. *Beck*, 848 F.3d at 275. A "highly attenuated chain of possibilities" in which the Court must make a series of assumptions to find a threatened injury "cannot confer standing." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013); *Beck*, 848 F.3d at 275. "Moreover, as the breaches fade further into the past, the [p]laintiffs' threatened injuries become more and more speculative." *Id.* (internal quotation omitted). The cost of mitigative measures, or "self-imposed harms,

cannot confer standing." *Id.* at 276-77; *see also Clapper*, 568 U.S. at 402 (rejecting the respondents' contention of "present injury because the risk of § 1881a-authorized surveillance already has forced them to take costly and burdensome measures to protect the confidentiality of their international communications" and finding that "respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending"). Without an imminent threat, "the cost of measures to guard against identity theft, including the cost of credit monitoring services . . . do[es] not constitute an injury-in-fact." *Beck*, 848 F.3d at 276.

Second, standing requires a causal connection between the alleged injury and the defendant's action. "[T]he 'case or controversy' limitation of Art[icle] III still requires that a federal court act only to redress injury that fairly can be traced to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court." *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41-42, 96 S. Ct. 1917, 48 L. Ed. 2d 450 (1976).

Finally, "there must be redressability—a likelihood that the requested relief will redress the alleged injury." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103, 118 S. Ct. 1003, 140 L. Ed. 2d 210 (1998). "[T]he point has always been the same: whether a plaintiff 'personally would benefit in a tangible way from the court's intervention.'" *Id.* at n.5 (quoting *Warth v. Seldin*, 422 U.S. 490, 508, 95 S. Ct. 2197, 45 L. Ed. 2d 343 (1975)).

When a plaintiff seeks injunctive relief, she must still establish each element of standing but the injury-in-fact requirement for standing differs slightly. "[A] plaintiff can satisfy the injury-in-fact requirement for prospective relief either by demonstrating a sufficiently imminent injury in fact or by demonstrating an ongoing injury." *Garey*, 35 F.4th at 922 (quoting *Deal v. Mercer Cnty. Bd. of Educ.*, 911 F.3d 183, 189 (4th Cir. 2018)) (internal quotation omitted) (alteration in the original). "[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion LLC*, 141 S. Ct. at 2210. The Fourth Circuit has "decline[d] to infer a substantial risk of harm of future identity theft from an organization's offer to provide free credit monitoring services to affected individuals." *Beck*, 848 F.3d at 276.

III. DISCUSSION

Bias, Cardenas, and Shaw do not allege a concrete and particularized injury-in-fact to establish Article III standing. Holmes does allege a cognizable injury but cannot fairly trace that injury to Elephant. The named plaintiffs therefore lack standing to assert claims for monetary damages (Counts One through Seven). Because none of the plaintiffs have alleged a substantial risk of imminent harm, they also lack standing to assert a claim for declaratory and injunctive relief (Count Eight). Because the Court therefore lacks jurisdiction over this action, the Court will not reach the merits of the plaintiffs' claims.

Appendix B

A. Standing — Monetary Damages (Counts One Through Seven)

1. Injury-in-Fact

The plaintiffs allege the following injuries: (1) "be[ing] at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages for years to come[;]" (2) identity theft (as demonstrated by one's "driver's license number [being] for sale on the dark web"); (3) "loss of privacy[;]" (4) "significant fear, anxiety, and stress[;]" (5) diminution in the value of their PI; and (6) "time reviewing [their] bank statements, tax information, car titles, and credit card statements." (ECF No. 18 ¶¶ 83, 88, 92-93, 97, 101-03, 190.)

a. Heightened Risk of Future Identity Theft

The heightened risk of future identity theft, without more, does not constitute an injury-in-fact because a "threatened injury must be certainly impending to constitute an injury-in-fact." *Clapper*, 568 U.S. at 410 (internal quotation omitted). Although the plaintiffs closely monitor their credit reports and financial accounts, none have alleged misuse of their PI. None have pleaded facts to support their allegations of certainly impending identity theft. In fact, "as the breaches fade further into the past, the [p]laintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275. The *Clapper* Court rejected the "highly attenuated chain of possibilities" required to show a threatened injury conferring standing. *Clapper*, 568 U.S. at 410. In this case,

to find a threatened injury, the Court must assume that the thief targeted Elephant for the PI it contained, then selected the named plaintiffs' PI from millions of other records, has begun combining the purloined PI with PI obtained from other sources to create a full profile (or "fullz"[3], and will imminently and successfully attempt to use that information to steal the plaintiffs' identities. In *Beck*, the Fourth Circuit rejected an even shorter chain of possibilities to deny the plaintiffs standing on a claim of heightened risk of identity theft. *Beck*, 848 F.3d at 276. Because the Fourth Circuit has rejected even shorter chains of possibilities, that the plaintiffs have here not adequately pleaded a heightened risk of identity sufficient to confer standing.

b. Identity Theft

Only two of the named plaintiffs have alleged identity theft. Cardenas and Holmes report receiving notifications from a credit monitoring service that their driver's license numbers appeared on the dark web. As the plaintiffs themselves allege, "a driver's license [number] *combined* with the full name and state issued, is a sought-after data point." (ECF No. 18 ¶ 32 (emphasis added).)[4] The driver's license number's real value lies in being pieced together

3. The plaintiffs note that "'[f]ullz' is slang used by threat actors and various criminals meaning 'full information,' a complete identity profile or set of information on any entity or individual." (ECF No. 18, at 12 n.19.)

4. The plaintiffs do not allege that the Data Breach included the issuing state for the plaintiffs' driver's licenses.

with other PI to create a full profile. "[H]ackers often aggregate information taken from data breaches on users to build profiles on individuals" because "[t]here are few data breaches that provide a comprehensive snapshot of any one individual person." (*Id.* ¶ 30.) To derive value from a driver's license number (and thus harm the plaintiffs), identity thieves would have to already possess other key pieces of these plaintiffs' PI or search the dark web for this PI, find enough pieces to create full profiles, then either use the full profiles themselves or sell them on the dark web to downstream actors who would use them for nefarious purposes. Because the plaintiffs have not alleged any misuse of their PI or resulting harm from the their driver's license numbers appearing on the dark web, this alleged injury simply echoes the claim of heightened risk of identity theft. The plaintiffs have not adequately pleaded an injury-in-fact.

c. Loss of Privacy

The loss of privacy can constitute an injury-in-fact. *See Garey*, 35 F.4th at 921. Only Holmes alleges facts amounting to a cognizable loss of privacy. He alleges that he "began experiencing an uptick in spam text and telephone calls that he attributes to this Data Breach." (ECF No. 18 ¶ 97.) In *Garey*, the Fourth Circuit determined that receiving unsolicited mail from a law firm closely paralleled the tort of loss of privacy and recognized it as an injury-in-fact. *Garey*, 35 F.4th at 922. Spam texts and calls invade an individual's privacy as much or perhaps even more than unsolicited mail. Holmes has sufficiently pleaded an injury-in-fact.

d. Emotional Distress

Emotional distress does not constitute a cognizable injury-in-fact. *Beck*, 848 F.3d at 272 ("We also reject the [p]laintiffs' claim that emotional upset and fear of identity theft and identity fraud resulting from the data breaches are . . . sufficient to confer Article III standing." (internal quotations omitted)). In *Beck*, the Fourth Circuit affirmed the district court's dismissal for lack of standing and found that "'conclusory allegations' that [the plaintiff] was 'torn . . . all to pieces' by the unauthorized disclosure of his social security number" cannot "support . . . the proposition that bare assertions of emotional injury are sufficient to confer Article III standing." *Id.* at 273 (quoting *Doe v. Chao*, 540 U.S. 614, 617, 124 S. Ct. 1204, 157 L. Ed. 2d 1122 (2004)). Holmes avers that he suffers "significant fear, anxiety, and stress" resulting from the Data Breach. (ECF No. 18 ¶ 101.) Shaw too suffers "significant fear, anxiety, and stress." (*Id.* ¶ 114.) Neither plaintiff expands upon these conclusory allegations of emotional distress. Because the plaintiffs plead only "bare assertion of emotional injury," they have not pleaded an injury-in-fact. *Beck*, 848 F.3d at 273.

e. Loss of Value in PI

The plaintiffs claim the Data Breach caused their PI to diminish in value. (*Id.* ¶ 190.) They allege no facts to explain how their PI lost value and instead only repeat conclusory statements: the plaintiffs "have suffered and will continue to suffer . . . loss of value of their PI." (*Id.* ¶ 218.) On a 12(b)(1) motion, courts have declined to

find diminution of value in PI as an injury-in-fact when plaintiffs make only barebones assertions. *See In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 403 (E.D. Va. 2020) ("Nor is there any allegation that Plaintiff[s] have attempted to purchase goods or services, which requires the exchange of their PII, and Plaintiffs were denied receipt of that good or service or were only offered less-than-desirable terms because of their PII's prior exposure through the Data Breach.") Conversely, when plaintiffs allege that they had to take extra steps to receive approval for a low-interest credit card after a data breach, courts have found that they have plausibly alleged the lost value of their PI as an injury. *See McCreary v. Filters Fast LLC*, No. 3:20-cv-595-FDW-DCK, 2021 U.S. Dist. LEXIS 133608, 2021 WL 3044228, at *6 n.3 (W.D. N.C. July 19, 2021). Because the plaintiffs plead no facts to support their conclusory allegation that their PI lost value, the Court cannot find that they have alleged an injury-in-fact.

f. Mitigative Measures

Finally, the plaintiffs' time spent paying close attention to their financial documents following the Data Breach does not constitute an injury-in-fact. Even if the plaintiffs had alleged that they spent money on protective services, the Fourth Circuit has held that expenses incurred on preventative or mitigative measures do not constitute an injury. *Beck*, 848 F.3d at 276-77 ("self-imposed harms cannot confer standing"). As the Court discussed above, the threat of identity theft is neither imminent nor substantial. Without an imminent threat,

"the cost of measures to guard against identity theft . . . do[es] not constitute an injury in fact." *Beck*, 848 F.3d at 276. Because the Fourth Circuit has not accepted mitigative measures as an injury-in-fact, the Court must find that the plaintiffs have failed to establish an injury.

~ ~ ~

The Court will grant Elephant's motion and dismiss Counts One through Seven as to Bias, Cardenas, and Shaw because these plaintiffs have not adequately pleaded an injury-in-fact and therefore lack standing. Only Holmes alleges a cognizable injury-in-fact. But, for the below reasons, Holmes lacks standing because he cannot fairly trace the injury to Elephant.

2. Traceability

Holmes alleges that he "began experiencing an uptick in spam text and telephone calls that he attributes to this Data Breach." (ECF No. 18 ¶ 97.) He asserts he never requested an insurance quote from Elephant and alleges that an unauthorized actor used the online quote tool to retrieve his PI. The plaintiffs do not allege that the PI in this Data Breach included cell phone numbers. To the extent Holmes claims a loss of privacy due to the "uptick in spam text and telephone calls," he has not pleaded any facts that causally connect this uptick in spam to Elephant. (*Id.* ¶ 97.) Holmes has failed to adequately allege traceability and therefore lacks standing to assert Counts One through Seven.

Appendix B

B. Standing — Declaratory and Injunctive Relief (Count Eight)

"[A] plaintiff must 'demonstrate standing separately for each form of relief sought.'" *TransUnion LLC*, 141 S. Ct. at 2208 (quoting *Friends of the Earth, Inc. v. Laidlaw Env'tal Svcs. (TOG), Inc.*, 528 U.S. 167, 185, 120 S. Ct. 693, 145 L. Ed. 2d 610 (2000)). The injury-in-fact requirement to seek monetary damages differs from the injury-in-fact requirement to seek injunctive relief. "[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Id.*

The plaintiffs ask the Court to declare that Elephant's "existing security measures do not comply with their duties of care to provide adequate security." (ECF No. 18 ¶ 254.) They further ask the Court to order Elephant to "implement and maintain reasonable security measures." (*Id.*) The plaintiffs allege, without factual support, that "[t]he risk of another such disclosure is real, immediate, and substantial." (*Id.* ¶ 255.) Because the plaintiffs have made only conclusory statements and have not articulated a sufficiently imminent and substantial risk of another Elephant data breach, the Court finds the plaintiffs lack standing to seek declaratory and injunctive relief. The Court will grant Elephant's motion and dismiss Count Eight.

~ ~ ~

In sum, the plaintiffs lack standing as to all Counts, and the Court must dismiss the complaint.[5]

IV. CONCLUSION

The plaintiffs have not adequately pleaded facts to establish an injury-in-fact or traceability. Because the plaintiffs lack standing to bring claims for monetary damages, the Court will grant Elephant's motion and dismiss Counts One through Seven. Further, because the plaintiffs have not alleged facts showing that a second Data Breach is imminent or substantial, they lack standing to bring a claim for declaratory and injunctive relief. Accordingly, the Court will grant Elephant's motion and dismiss Count Eight.

The Court will issue an appropriate Order.

Let the Clerk send a copy of this Opinion to all counsel of record.

Date: 26 June 2023
Richmond, VA

/s/ John A. Gibney, Jr.
John A. Gibney, Jr.
Senior United States District Judge

5. Because the plaintiffs lack standing to assert their claims, the Court will not reach Elephant's arguments regarding failure to state a claim.

APPENDIX C — ORDER OF THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, RICHMOND DIVISION, FILED JUNE 26, 2023

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

Civil Action No. 3:22cv487

CHRISTOPHER HOLMES *et al.*, ON BEHALF OF THEMSELVES AND ALL SIMILARLY SITUATED PERSONS,

Plaintiffs,

v.

ELEPHANT INSURANCE COMPANY, *et al.*,

Defendants.

ORDER

This matter comes before the Court on the defendants' motion to dismiss the plaintiffs' consolidated class action complaint. (ECF No. 27.) For the reasons stated in the accompanying Opinion, the Court GRANTS the defendants' motion and DISMISSES the complaint. Accordingly, the Court DIRECTS the Clerk to close this case.

It is so ORDERED.

Let the Clerk send a copy of this Order to all counsel of record.

Date: 26 June 2023
Richmond, VA

/s/ John A. Gibney, Jr.
John A. Gibney, Jr.
Senior United States District Judge