PUBLISHED

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.

ARGUED: Kate M. Baxter-Kauf, LOCKRIDGE, GRINDAL & NAUEN, P.L.L.P., Minneapolis, Minnesota, for Appellants. James Francis Monagle, MULLEN COUGHLIN LLC, Sacramento, California, for Appellees. **ON BRIEF:** Lee Floyd, BREIT BINIAZAN, PC, Richmond, Virginia; M. Anderson Berry, CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP., Sacramento, California; Gayle M. Blatt, CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP, San Diego, California;

David K. Lietz, MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC, Washington, D.C., for Appellants. Claudia D. McCarron, MULLEN COUGHLIN LLC, Devon, Pennsylvania, for Appellees.

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]

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

[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 (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.

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.*, 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 and dismissed the entire case. *Id.* 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 (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 (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 (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 (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 (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 (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]

---

[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 WL

(Continued)

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

---

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.*

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 potential terrorists and criminals—had suffered a harm sufficiently close to that inflicted by defamation. 594 U.S.

[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.

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" 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.

[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.*

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

[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.

[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").

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 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 Publ'ns., Inc. v. Hitchner*, 549 So.2d 1374, 1377 (Fla. 1989); *Shulman v. Grp W. Prods., Inc.*, 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

---

[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*, 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 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.

(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 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 (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 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

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

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-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

[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).

[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.

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 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

[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.

[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.

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 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,

[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.

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] 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

[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 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).

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.

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 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 (2013). Instead, "the plaintiffs must show a

[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.

substantial risk that" it will happen "in the near future." *Murthy v. Missouri*, 603 U.S. 43, 58 (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 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

[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 (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.

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 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 (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

[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 (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.

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; 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 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

[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.

[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 (Continued)

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 "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.

---

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.

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 (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 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

[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 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 (2012) (explaining that "special damages" are "actual pecuniary loss[es]" that are incurred from an invasion of privacy (quotation omitted)).

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. *Fed. Election Comm'n v. Cruz*, 596 U.S. 289, 297 (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]

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

[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, 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.

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, 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.