United States Court of Appeals
For the First Circuit

No. 22-1896

ALEXSIS WEBB, on behalf of herself and all others similarly situated; MARSCLETTE CHARLEY, on behalf of herself and all others similarly situated,

Plaintiffs, Appellants,

v.

INJURED WORKERS PHARMACY, LLC,

Defendant, Appellee.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

[Hon. Richard G. Stearns, U.S. District Judge]

Before

Kayatta, Lynch, and Montecalvo,
Circuit Judges.

David K. Lietz, with whom Milberg Coleman Bryson Phillips Grossman, PLLC, Raina C. Borrelli, and Turke & Strauss, LLP were on brief, for appellants.

Claudia D. McCarron, with whom Jordan S. O'Donnell and Mullen Coughlin LLC were on brief, for appellee.

June 30, 2023

LYNCH, Circuit Judge. Named plaintiffs Alexsis Webb and Marsclette Charley brought this putative class action against defendant Injured Workers Pharmacy, LLC ("IWP"), asserting various state law claims in relation to a January 2021 data breach that allegedly exposed their personally identifiable information ("PII") and that of over 75,000 other IWP patients. The district court concluded that the plaintiffs' complaint did not plausibly allege an injury in fact and dismissed the case for lack of Article III standing. See Webb v. Injured Workers Pharmacy, LLC, No. 22-cv-10797, 2022 WL 10483751, at *2 (D. Mass. Oct. 17, 2022).

We hold that the complaint plausibly demonstrates the plaintiffs' standing to seek damages. The plaintiffs press five causes of action seeking damages, each of which encompasses at least one of the harms that we hold satisfy the requirements of Article III standing. The complaint plausibly alleges an injury in fact as to Webb based on the allegations of actual misuse of her PII to file a fraudulent tax return. Further, the complaint plausibly alleges an injury in fact as to both plaintiffs based on an imminent and substantial risk of future harm as well as a present and concrete harm resulting from the exposure to this risk. We also hold that the plaintiffs lack standing to pursue injunctive relief because their desired injunctions would not likely redress their alleged injuries. We affirm in part, reverse in part, and remand for further proceedings.

I.

A.

We recount the facts as they appear in the plaintiffs' complaint and in documents attached to the complaint or incorporated therein. Hochendoner v. Genzyme Corp., 823 F.3d 724, 728 (1st Cir. 2016).

IWP is a home-delivery pharmacy service registered and headquartered in Massachusetts. It maintains records of its patients' full names, Social Security numbers, and dates of birth, as well as information concerning their financial accounts, credit cards, health insurance, prescriptions, diagnoses, treatments, healthcare providers, and Medicare/Medicaid IDs. Much of this information constitutes PII. See, e.g., United States v. Cruz-Mercedes, 945 F.3d 569, 572 (1st Cir. 2019). Patients provided their PII in order to receive IWP's services, and IWP kept that PII. IWP represented to patients that it would keep their PII secure.

In January 2021, IWP suffered a data breach. Hackers infiltrated IWP's patient records systems, gaining access to the PII of over 75,000 IWP patients, and stole PII including patient names and Social Security numbers.[1] IWP did not discover this

[1] IWP stated in a notice letter to potentially impacted patients that "an unknown actor accessed a total of seven . . . IWP e-mail accounts" over a four-month period. The complaint alleges that hackers "infiltrated IWP's patient records systems."

breach until May 2021, almost four months later. In the interim, the hackers were able to continue accessing PII. On learning of the breach, IWP did not immediately alert its patients. Instead, it initiated a seven-month investigation and worked to implement new data security safeguards.

IWP did not begin notifying impacted patients until February 2022, when it circulated a notice letter. This notice provided a high-level description of the breach but, in the plaintiffs' view, did not fully convey its size or scope. The notice stated that IWP "currently ha[d] no evidence that any information ha[d] been misused." It also "encourage[d] [patients] to . . . review[] [their] account statements and monitor[] [their] credit reports for suspicious activity" and referred patients to a guidance document on protecting their personal information. IWP has not offered to provide, at its own expense, credit monitoring and identity protection services to all impacted patients.

Alexsis Webb is a former IWP patient who received services from IWP between 2017 and 2020. She is a resident of Ohio. In February 2022, IWP notified her that her PII had been compromised in the data breach. As a result, Webb allegedly "fears for her personal financial security and [for] what information was

---

The plaintiffs appear to agree that the "initial attack vector" was into IWP employee email accounts but contend that this allowed the hackers to access additional system information.

revealed in the [d]ata [b]reach," "has spent considerable time and effort monitoring her accounts to protect herself from . . . identity theft," and "is experiencing feelings of anxiety, sleep disruption, stress, and fear" because of the breach. Webb's PII was used to file a fraudulent 2021 tax return, and she has "expended considerable time" communicating with the Internal Revenue Service ("IRS") to resolve issues associated with this false return.

Marsclette Charley is a current IWP patient who has received services from IWP since 2016. She is a resident of Georgia. Like Webb, she became aware in February 2022 that her PII had been compromised in the breach. She called IWP to confirm that her information was stolen, but IWP's representatives would not provide her with specific details as to what types of information were accessed. As a result of the breach, Charley allegedly "fears for her personal financial security," "expends considerable time and effort monitoring her accounts to protect herself from . . . identity theft," and "is experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain."

B.

On May 24, 2022, Webb and Charley filed a class action complaint against IWP in the U.S. District Court for the District of Massachusetts, invoking the court's jurisdiction under the

Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The complaint asserts state law claims for negligence, breach of implied contract, unjust enrichment, invasion of privacy, and breach of fiduciary duty.[2] The complaint seeks damages, an injunction "[e]njoining [IWP] from further deceptive and unfair practices and making untrue statements about the [d]ata [b]reach and the stolen PII," other injunctive and declaratory relief "as is necessary to protect the interests of [the] [p]laintiffs and the [c]lass," and attorneys' fees. It seeks to certify a class of U.S. residents whose PII was compromised in the data breach.

On August 9, 2022, IWP moved to dismiss the complaint on two bases: under Federal Rule of Civil Procedure ("Rule") 12(b)(1), for lack of Article III standing, and under Rule 12(b)(6), for failure to state a claim as to each of the complaint's asserted claims. The plaintiffs opposed the motion.

On October 17, 2022, the district court granted IWP's motion and dismissed the case under Rule 12(b)(1). Webb, 2022 WL 10483751, at *2. The court concluded that the plaintiffs lacked Article III standing because their complaint did not plausibly allege an injury in fact. Id. As to the complaint's allegation that a fraudulent tax return was filed in Webb's name, the court

[2] The complaint also asserts a state law claim for negligence per se. The plaintiffs agreed to voluntarily dismiss this claim in their district court briefing.

reasoned that the complaint did not sufficiently allege a connection between the data breach and this false return. See id. at *2 n.4. As to the complaint's other allegations, the court reasoned that the potential future misuse of the plaintiffs' PII was not sufficiently imminent to establish an injury in fact and that actions to safeguard against this risk could not confer standing either. See id. at *2. Because it dismissed the case under Rule 12(b)(1), the court did not reach IWP's Rule 12(b)(6) arguments. Id. at *1 n.2.

This timely appeal followed.

II.

The plaintiffs' complaint must meet standing requirements based on Article III of the Constitution, which limits "[t]he judicial Power" to "Cases" and "Controversies." U.S. Const. art. III, § 2, cl. 1; see In re: Evenflo Co., Inc., Mktg., Sales Pracs. & Prods. Liab. Litig., 54 F.4th 28, 34 (1st Cir. 2022). "The existence of standing is a legal question, which we review de novo." Evenflo, 54 F.4th at 34 (quoting Kerin v. Titeflex Corp., 770 F.3d 978, 981 (1st Cir. 2014)). "When reviewing a pre-discovery grant of a motion to dismiss for lack of standing, we accept as true all well-pleaded fact[s] . . . and indulge all reasonable inferences in the plaintiff[s'] favor." Id. (alterations and omission in original) (internal quotation marks omitted) (quoting Kerin, 770 F.3d at 981). "[W]e apply the same

plausibility standard used to evaluate a motion under Rule 12(b)(6)." Gustavsen v. Alcon Lab'ys, Inc., 903 F.3d 1, 7 (1st Cir. 2018). At this stage in the proceedings, our analysis focuses on whether the two named plaintiffs have standing. See id.; Hochendoner, 823 F.3d at 730, 733-34; 1 W. Rubenstein, Newberg and Rubenstein on Class Actions §§ 2:1, 2:3 (6th ed. June 2023 update).

"[P]laintiffs bear the burden of demonstrating that they have standing," TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2207 (2021), and must do so "with the manner and degree of evidence required at the successive stages of the litigation," id. at 2208 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992)). Plaintiffs "must demonstrate standing for each claim that they press and for each form of relief that they seek." Id. "To establish standing, a plaintiff must show an injury in fact caused by the defendant and redressable by a court order." United States v. Texas, No. 22-58, slip op. at 4 (U.S. June 23, 2023); see Evenflo, 54 F.4th at 34.

At issue in this appeal is the "injury in fact" requirement -- and, in particular, the requirement that this injury be "concrete." "[T]raditional tangible harms, such as physical harms and monetary harms" are "obvious[ly]" concrete. TransUnion, 141 S. Ct. at 2204. Intangible harms can also be concrete, including when they "are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits

in American courts," such as "reputational harms, disclosure of private information, and intrusion upon seclusion." Id.; see also Spokeo, Inc. v. Robins, 578 U.S. 330, 340-41 (2016). This "inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury," but "does not require an exact duplicate." TransUnion, 141 S. Ct. at 2204.

"[A] material risk of future harm can [also] satisfy the concrete-harm requirement," but only as to injunctive relief, not damages. Id. at 2210; see id. at 2210-11. To have standing to pursue damages based on a risk of future harm, plaintiffs must demonstrate a separate concrete harm caused "by their exposure to the risk itself." Id. at 2211.

Applying these principles in TransUnion, the Supreme Court concluded that only a portion of the certified class in that case had standing to pursue the claim that TransUnion, a credit reporting agency, had failed to use reasonable procedures in maintaining its credit files. See id. at 2200, 2208. The class comprised individuals whose TransUnion credit reports bore alerts erroneously suggesting that they might be terrorists or other serious criminals. Id. at 2201-02. The Court held that the 1,853 class members whose credit reports TransUnion disseminated to third parties had standing, because this injury bore a sufficiently close relationship to "the reputational harm associated with the tort of defamation." Id. at 2208. That the credit reports "were

only misleading and not literally false" did not defeat standing, because "an exact duplicate" of a traditionally recognized harm is not required. Id. at 2209.

However, the remaining 6,332 class members whose credit reports were not disseminated to third parties lacked standing. Id. at 2212. The Court first considered whether the mere existence of misleading alerts in these plaintiffs' internal TransUnion credit files (absent dissemination) was a concrete injury and concluded that it was not. See id. at 2209-10. The Court then rejected the plaintiffs' effort to establish standing for damages on a risk of future harm theory, reasoning that they had not demonstrated that they "were independently harmed by their exposure to the risk itself -- that is, that they suffered some other injury . . . from the mere risk that their credit reports would be provided to third-party businesses." Id. at 2211; see id. at 2210-11. The Court noted that emotional harm might supply the requisite concrete, present injury but did not reach this question because the plaintiffs had not claimed any such injury. See id. at 2211 & n.7.

III.

A.

We begin with Webb's standing to pursue damages. We conclude that the complaint plausibly alleges a concrete injury in fact as to Webb based on the plausible pleading that the data

breach resulted in the misuse of her PII by an unauthorized third party (or third parties) to file a fraudulent tax return.[3]

Our data security precedents support the conclusion that actual misuse of PII may constitute an injury in fact. In Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012), we concluded that the named plaintiff lacked standing to sue as to her state law consumer protection claims that the defendant had employed inadequate data security practices. See id. at 69-70. We stated that "[c]ritically, the complaint [did] not contain an allegation that [her] nonpublic personal information ha[d] actually been accessed by any unauthorized user" -- let alone subsequently misused -- but rather "rest[ed] entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity." Id. at 79. The alleged harm in that case was not "impending" because it was "unanchored to any actual incident of data breach." Id. at 80. And the plaintiff could not manufacture standing by incurring mitigation costs in the absence of an impending harm. See id. at

[3] The claims asserted in the plaintiffs' complaint all arise from the IWP data breach, and neither party argues that the standing inquiry differs with respect to any claim. Accordingly, we treat the claims together throughout our analysis. See TransUnion, 141 S. Ct. at 2213-14 (assessing standing for "intertwined" claims together); Evenflo, 54 F.4th at 35 (similar); Clemens v. ExecuPharm Inc., 48 F.4th 146, 156-59 (3d Cir. 2022) (employing same underlying standing analysis for contract, tort, and "secondary contract" claims in data breach case).

79. We distinguished the case from those "in which confidential data actually has been accessed through a security breach and persons involved in that breach have acted on the ill-gotten information." Id. at 80 (emphasis added).[4]

We hold that the complaint's plausible allegations of actual misuse of Webb's stolen PII to file a fraudulent tax return suffice to state a concrete injury under Article III. This conclusion accords with the law of other circuits. See, e.g., In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1262 (11th Cir. 2021) (identifying both "identity theft and damages resulting from such theft" as concrete injuries); Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017) ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.").

[4] Our decision in Anderson v. Hannaford Brothers Co., 659 F.3d 151 (1st Cir. 2011), is also instructive. To be clear, Anderson did not concern Article III standing. It did, however, discuss the types of harms that can arise out of data misuse following a data breach. Id. at 162-67. In that case, we reversed the district court's dismissal of certain state law claims because the plaintiffs' alleged mitigation costs were incurred in response to a serious data breach and actual misuse of PII and were thus "reasonable" and "constitute[d] a cognizable harm under Maine law." Id. at 154, 164; see id. at 162-67. The data breach involved "the deliberate taking of credit and debit card information by sophisticated thieves" and the "actual misuse" of this information to "run up thousands of improper charges across the globe." Id. at 164; see id. at 154. We concluded that "[t]he [plaintiffs] were not merely exposed to a hypothetical risk, but to a real risk of misuse." Id. at 164.

The district court concluded that the complaint did not plausibly allege a connection between the data breach and the filing of the false tax return. See Webb, 2022 WL 10483751, at *2 n.4. We disagree. In our view, the complaint plausibly alleges a connection between the actual misuse of Webb's PII and the data breach. In applying the plausibility standard required at the motion to dismiss stage, we "[must] draw on [our] judicial experience and common sense . . . [and] read [the complaint] as a whole." Evenflo, 54 F.4th at 39 (alterations and omission in original) (internal quotation marks omitted) (quoting García-Catalán v. United States, 734 F.3d 100, 103 (1st Cir. 2013)). We must also "indulge all reasonable inferences in the plaintiff[s'] favor." Id. at 34 (alteration in original) (internal quotation marks omitted) (quoting Kerin, 770 F.3d at 981).

There is an obvious temporal connection between the filing of the false tax return and the timing of the data breach. Further, the complaint's allegation that Webb's PII was "used by an unauthorized individual" to file a false tax return is made in the context of allegations relating to harms Webb has suffered because of the data breach. The complaint also alleges that Webb is "very careful about sharing her PII," "has never knowingly transmitted unencrypted PII over the internet or any other unsecured source," and stores documents containing her PII in a secure location. The obvious inference to be drawn from these

allegations is that the criminal or criminals who filed the false tax return obtained Webb's PII from the IWP data breach, not from some other source. And the complaint alleges that, as a result of the data breach and IWP's conduct, the plaintiffs "have suffered or are at an increased risk of suffering . . . [d]elay in receipt of tax refund monies . . . [and the] [u]nauthorized use of stolen PII." These general allegations provide further support for a plausible connection. See In re: SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 772 (8th Cir. 2017) (holding that, at the motion to dismiss stage, a complaint's "'general allegations embrace[d] those specific facts . . . necessary to support' a link between [a plaintiff's] fraudulent charge and the data breaches" (quoting Bennett v. Spear, 520 U.S. 154, 168 (1997))).

We reject IWP's argument that the alleged actual misuse is not itself a concrete injury absent even more resulting harm to Webb. As described above, we agree with those courts that consider actual misuse of a plaintiff's PII resulting from a data breach to itself be a concrete injury. See, e.g., Equifax, 999 F.3d at 1262; Attias, 865 F.3d at 627. And beyond that, applying a TransUnion analysis, this alleged actual misuse is closely related to the tort of invasion of privacy based on appropriation of another's name or likeness, which "protect[s] . . . the interest of the individual in the exclusive use of his own identity, in so far as

it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others." Restatement (Second) of Torts § 652C cmt. a (Am. L. Inst. 1977); see id. § 652C cmt. b (noting that while some states have "limited . . . liability [by statute] to commercial uses of the name or likeness," the general rule is "not limited to commercial appropriation"); see also 141 S. Ct. at 2204.

B.

Charley's standing to pursue damages is more difficult. The complaint does not allege actual misuse of Charley's PII. Nonetheless, we conclude that, in light of the plausible allegations of some actual misuse, the complaint plausibly alleges a concrete injury in fact based on the material risk of future misuse of Charley's PII and a concrete harm caused by exposure to this risk.[5] This analysis is equally applicable to Webb and provides an independent basis for our conclusion that the complaint plausibly demonstrates standing as to Webb.

---

[5] The plaintiffs do not argue that the exposure of their PII in the breach was itself an intangible harm sufficient to confer standing -- for example, by analogy to the torts of breach of confidence or invasion of privacy based on public disclosure of private information. Cf. TransUnion, 141 S. Ct. at 2209 (analyzing similar "initial question" before turning to the plaintiffs' risk of future harm theory). Accordingly, we do not consider this question. And to the extent the plaintiffs seek to establish standing based on an alleged "diminution [in] value" of their PII, they have waived this argument by raising it for the first time in their reply brief. See, e.g., United States v. Abdelaziz, No. 22-1129, 2023 WL 3335870, at *41 n.36 (1st Cir. May 10, 2023).

1.

"[A] material risk of future harm can satisfy the concrete-harm requirement," at least as to injunctive relief, when "the risk of harm is sufficiently imminent and substantial." TransUnion, 141 S. Ct. at 2210; see also Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013).

Many of the same factors we have considered in other data breach cases inform our conclusion as to standing in this case. Plaintiffs face a real risk of misuse of their information following a data breach when their information is deliberately taken by thieves intending to use the information to their financial advantage -- i.e., exposed in a targeted attack rather than inadvertently. And the actual misuse of a portion of the stolen information increases the risk that other information will be misused in the future.

We stress that these considerations are neither exclusive nor necessarily determinative, but they do provide guidance. See, e.g., McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 302 (2d Cir. 2021) ("[D]etermining standing is an inherently fact-specific inquiry . . . ."). These considerations accord with other circuits' approach to determining when the risk of future misuse of PII following a data breach is imminent and substantial. The Second Circuit considers:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Id. at 303; see also id. at 300-03 (explaining the relevance of these factors).[6] The Third Circuit also considers these factors. See Clemens v. ExecuPharm Inc., 48 F.4th 146, 153-54, 157 (3d Cir. 2022). Both circuits emphasize that these factors are "non-exhaustive." McMorris, 995 F.3d at 303; Clemens, 48 F.4th at 153. Other circuits look to similar considerations. See McMorris, 995 F.3d at 300-03 (collecting cases and synthesizing principles).

It stands to reason that data compromised in a targeted attack is more likely to be misused. See Anderson, 659 F.3d at 164; see also, e.g., McMorris, 995 F.3d at 301; Clemens, 48 F.4th at 153; Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015); In re Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1029 n.13 (9th Cir. 2018); In re:

[6] McMorris and many of the other circuit cases discussed below were decided before TransUnion. Nevertheless, we think the factors the Second Circuit listed remain relevant to assessing the risk of future PII misuse. See Clemens v. ExecuPharm Inc., 48 F.4th 146, 153-54, 157 (3d Cir. 2022) (citing McMorris and applying similar factors post-TransUnion).

U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58-59 (D.C. Cir. 2019) ("OPM").

That at least some information stolen in a data breach has already been misused also makes it likely that other portions of the stolen data will be similarly misused. See Anderson, 659 F.3d at 164; see also, e.g., McMorris, 995 F.3d at 301-02; Remijas, 794 F.3d at 693-94; Zappos.com, 888 F.3d at 1027 n.7; OPM, 928 F.3d at 58-59.

And the risk of future misuse may be heightened where the compromised data is particularly sensitive. "Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth -- especially when accompanied by victims' names -- makes it more likely that those victims will be subject to future identity theft or fraud." McMorris, 995 F.3d at 302; see also Clemens, 48 F.4th at 154; OPM, 928 F.3d at 49, 59; Attias, 865 F.3d at 628. In contrast, the risk of future misuse may be lower where the stolen data is "less sensitive, . . . such as basic publicly available information, or data that can be rendered useless to cybercriminals." McMorris, 995 F.3d at 302; see also Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1343 (11th Cir. 2021) (emphasizing fact that plaintiff did not allege that his Social Security number or date of birth were compromised in data breach); SuperValu, 870 F.3d at 770-71 (similar).

We hold that the totality of the complaint plausibly alleges an imminent and substantial risk of future misuse of the plaintiffs' PII. The complaint alleges that the data breach was the result of an attack by "cybercriminals" who "infiltrated IWP's patient records systems" and "stole[] PII." These hackers were, by IWP's own admission, able to compromise multiple employee email accounts and to remain undetected for almost four months. The complaint further alleges that at least some of the stolen PII has already been misused to file a fraudulent tax return in Webb's name. And the complaint alleges that the stolen PII "include[s] . . . patients' names and [S]ocial [S]ecurity numbers." We do not hold that individuals face an imminent and substantial future risk in every case in which their information is compromised in a data breach. But on the facts alleged here, the complaint has plausibly demonstrated such a risk.

2.

To establish standing to pursue damages, the complaint must also plausibly allege a separate concrete, present harm caused "by [the plaintiffs'] exposure to [this] risk [of future harm]." TransUnion, 141 S. Ct. at 2211. We conclude that the complaint has done so based on the allegations of the plaintiffs' lost time spent taking protective measures that would otherwise have been

put to some productive use.[7] See Compl. ¶¶ 13, 56 (alleging "opportunity costs" and "lost wages" associated with "the time and effort expended addressing . . . future consequences of the [d]ata [b]reach").

The complaint alleges that both plaintiffs spent "considerable time and effort monitoring [their] accounts to protect [themselves] from . . . identity theft." The complaint elsewhere identifies the harms of lost time as "[l]ost opportunity costs and lost wages." The loss of this time is equivalent to a monetary injury, which is indisputably a concrete injury. See id. at 2204; see also Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018) (Easterbrook, J.) (recognizing that the opportunity cost of "one's own time needed to set things straight" following a data breach "can justify money damages, just as [it] support[s] standing"); In re: Gen. Motors LLC Ignition Switch Litig., 339 F. Supp. 3d 262, 307 (S.D.N.Y. 2018) ("[T]he overwhelming majority of states adhere to the view that lost-time damages are the equivalent of lost earnings or income.").[8] We join

[7] The complaint does not allege that Webb or Charley purchased identity theft insurance or credit monitoring services or incurred similar mitigation costs. See TransUnion, 141 S. Ct. at 2204; see also, e.g., Clemens, 48 F.4th at 156; Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018).

[8] Because we conclude that the complaint plausibly alleges the loss of time that would otherwise have been put to profitable use, we do not consider whether the loss of personal time is either a tangible injury or an intangible injury with a "close historical

other circuits in concluding that time spent responding to a data breach can constitute a concrete injury sufficient to confer standing, at least when that time would otherwise have been put to profitable use. See, e.g., Clemens, 48 F.4th at 158; Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018); Galaria, 663 F. App'x at 388-89; Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016); Equifax, 999 F.3d at 1262.

Because this alleged injury was a response to a substantial and imminent risk of harm, this is not a case where the plaintiffs seek to "manufacture standing by incurring costs in anticipation of non-imminent harm." Clapper, 568 U.S. at 422; see also, e.g., McMorris, 995 F.3d at 303; Hutton, 892 F.3d at 622.

c.

The complaint's allegations also satisfy the traceability and redressability standing requirements. The complaint alleges that IWP's actions led to the exposure and actual or potential misuse of the plaintiffs' PII, making their injuries fairly traceable to IWP's conduct. See Evenflo, 54 F.4th at 41; Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of

---

or common-law analogue." TransUnion, 141 S. Ct. at 2204; cf. Gen. Motors LLC, 339 F. Supp. 3d at 307 ("[M]ost states do not treat lost personal time as a compensable form of injury.").

Article III standing, which requires only that the plaintiff's injury be fairly traceable to the defendant's conduct."). "And monetary relief would compensate [the plaintiffs] for their injur[ies], rendering the injur[ies] redressable." Evenflo, 54 F.4th at 41.

D.

Defendants do not contend that the plaintiffs' ability to pursue emotional distress as a specific category of damages presents an independent Article III standing issue even after plaintiffs have shown an actual injury supporting their claim for damages generally under each cause of action, and for good reason. "It is firmly established in our cases that the absence of a valid . . . cause of action does not implicate subject-matter jurisdiction, i.e., the courts' statutory or constitutional power to adjudicate the case." Steel Co. v. Citizens for a Better Environment, 523 U.S. 83, 89 (1998). On the appeal before us we consider only whether the plaintiffs have "demonstrate[d] standing for each claim that they press and for each form of relief that they seek." TransUnion, 141 S.Ct. at 2208. Having concluded that plaintiffs have supported each of their five causes of action for damages with at least one injury in fact caused by the defendant and redressable by a court order, we venture no further. Cf. Attias, 865 F.3d at 626 n.2 (declining to address standing based on past identity theft because the risk of future identity theft,

along with associated mitigation expenses, sufficed to confer standing); Linman v. Marten Transp., Ltd., No. 22-CV-204-JDP, 2023 WL 2562712, at *3 (W.D. Wis. Mar. 17, 2023) (finding time spent mitigating the risk of identity theft sufficient for standing and declining to decide whether other alleged injuries such as emotional distress are sufficient); TransUnion, 141 S. Ct. at 2211 & n.7. Whether the plaintiffs have stated a claim for damages specifically arising out of their emotional distress is a question for IWP's 12(b)(6) motion which, as discussed below, we do not reach.

IV.

We next consider the plaintiffs' standing to seek injunctive relief. We conclude that the plaintiffs lack standing to pursue such relief because their requested injunctions are not likely to redress their alleged injuries. See Lujan, 504 U.S. at 568-71.

The only allegation in the complaint that injunctive relief is necessary is that plaintiffs' "PII [is] still maintained by [IWP] with [its] inadequate cybersecurity system and policies." Naturally, an injunction requiring IWP to improve its cybersecurity systems cannot protect the plaintiffs from future misuse of their PII by the individuals they allege now possess it. Any such relief would safeguard only against a future breach.

But the plaintiffs do not allege that any such future breach will occur. "Standing for injunctive relief depends on 'whether [the plaintiffs are] likely to suffer future injury.'" Laufer v. Acheson Hotels, LLC, 50 F.4th 259, 276 (1st Cir. 2022) (quoting City of Los Angeles v. Lyons, 461 U.S. 95, 105 (1983)). Here, any available inference that IWP's prior data breach might make a future data breach more likely is undercut by the plaintiffs' own allegation that "[f]ollowing the [d]ata [b]reach, IWP implemented new security safeguards to prevent and mitigate data breaches -- measures that should have been in place before the data breach." Instead, IWP faces much the same risk of future cyberhacking as virtually every holder of private data. If that risk were deemed sufficiently imminent to justify injunctive relief, virtually every company and government agency might be exposed to requests for injunctive relief like the one the plaintiffs seek here. We decline to hold as much. Because the plaintiffs have not shown that their requested injunction would likely redress their alleged injuries, they lack standing to pursue that form of relief. Cf. Lujan, 504 U.S. at 568-71.

The plaintiffs also request that the district court "[e]njoin[] [IWP] from further deceptive and unfair practices and making untrue statements about the [d]ata [b]reach and the stolen PII." But nowhere do the plaintiffs allege that IWP is likely to make deceptive statements about that past breach in the future or

that any such statements would harm the plaintiffs, particularly now that they know about the breach. Here, too, the plaintiffs' requested injunction would have no chance of redressing any alleged injury, and they lack standing to pursue it.

V.

We do not reach IWP's Rule 12(b)(6) arguments. The district court did not rule on these arguments, see Webb, 2022 WL 10483751, at *1 n.2, and will have the opportunity to do so in the first instance on remand, see, e.g., Evenflo, 54 F.4th at 41.

VI.

For the foregoing reasons, we affirm in part, reverse in part, and remand for further proceedings consistent with this opinion. No costs are awarded.