79 F.4th 276
United States Court of Appeals, Second Circuit.

Nancy BOHNAK, on behalf of themselves and all others similarly situated, Plaintiff-Appellant,
Janet Lea Smith, on behalf of themselves and all others similarly situated, Plaintiff,
v.
MARSH & MCLENNAN COMPANIES, INC., a Delaware Corporation, Marsh & McLennan Agency, LLC, a Delaware Limited Liability Company, Defendants-Appellees.

Docket No. 22-319
|
August Term, 2022
|
Submitted: October 24, 2022
|
Decided: August 24, 2023

Synopsis

Background: Former employee brought putative class action against employer and its parent after her personally identifying information (PII), including her name and Social Security number, which had been entrusted to defendants, were exposed to an unauthorized third party as a result of a targeted data hack, asserting state law claims of negligence, breach of implied contract, and breach of confidence. The United States District Court for the Southern District of New York, Hellerstein, J., 580 F.Supp.3d 21, granted defendants' motions to dismiss. Former employee appealed.

Holdings: The Court of Appeals, Robinson, Circuit Judge, held that:

[1] risk of future harm to former employee arising from disclosure of her PII was a cognizable concrete injury for Article III standing purposes;

[2] out-of-pocket expenses former employee incurred associated with prevention, detection, and recovery from identity theft was a concrete injury;

[3] former employee satisfied the actual or imminent harm component of the injury in fact element of Article III standing;

[4] former employee satisfied the particularity component of the injury in fact element of Article III standing; and

[5] former employee pled cognizable damages with reasonable certainty, as required to state her claims.

Reversed and remanded.

Procedural Posture(s): On Appeal; Motion to Dismiss for Failure to State a Claim; Motion to Dismiss for Lack of Subject Matter Jurisdiction.

West Headnotes (13)

[1] **Federal Civil Procedure** In general; injury or interest

Federal Civil Procedure Causation; redressability

To establish Article III standing under the United States Constitution, a plaintiff must show (1) an injury in fact (2) caused by the defendant, (3) that would likely be redressable by the court. U.S. Const. art. 3, § 2, cl. 1.

[2] **Federal Civil Procedure** In general; injury or interest

Injury in fact, for purposes of Article III standing, embodies three components: it must be concrete, particularized, and actual or imminent. U.S. Const. art. 3, § 2, cl. 1.

[3] **Federal Courts** Pleading

District court's order dismissing, for failure to state a claim, former employee's claims for negligence, breach of implied contract, and breach of confidence against employer and its parent arising from data hack that exposed her personally identifying information (PII) was appealable because it was a final decision that disposed of the entire case, though the better practice would have been for employee to appeal the judgment the district court subsequently entered, so as to avoid any dispute as to whether

the earlier entered order qualified as a final decision. 28 U.S.C.A. § 1291; Fed. R. Civ. P. 12(b)(6).

More cases on this issue

[4] **Federal Courts** Judgment or dismissal on the pleadings

Where Article III standing is challenged on the basis of the pleadings, the Court of Appeals accepts as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party. U.S. Const. art. 3, § 2, cl. 1.

1 Case that cites this headnote

[5] **Federal Courts** Standing

On appeal from the denial of a motion to dismiss due to lack of standing, the Court of Appeals determines whether a plaintiff has constitutional standing to sue without deference to the district court. U.S. Const. art. 3, § 2, cl. 1.

[6] **Labor and Employment** Parties in general; standing

The risk of future harm to former employee arising from disclosure of her personally identifying information (PII), including her name and Social Security number, to unauthorized third parties as a result of targeted data hack against her former employer was a cognizable concrete injury, as required for former employee to have Article III standing to bring negligence, breach of implied contract, and breach of confidence claims against her former employer and its parent; core of former employee's alleged injury was that she had been harmed by exposure of her private information to an unauthorized malevolent actor, this fell squarely within scope of a concrete intangible harm, and it bore some relationship to a well-established common-law analog, namely public disclosure of private facts. U.S. Const. art. 3, § 2, cl. 1.

2 Cases that cite this headnote
More cases on this issue

[7] **Telecommunications** Persons entitled to sue, standing, and parties

For the purposes of the "concreteness" analysis of the injury in fact element of Article III standing arising from the disclosure of the plaintiff's personally identifying information (PII), what matters is that the intangible harm arising from disclosure of one's PII bears a relationship to an injury with a close historical or common-law analogue, and that analog need not be an exact duplicate. U.S. Const. art. 3, § 2, cl. 1.

1 Case that cites this headnote

[8] **Labor and Employment** Parties in general; standing

The out-of-pocket expenses former employee incurred associated with the prevention, detection, and recovery from identity theft and lost time and other opportunity costs from attempting to mitigate the consequences of the data breach that exposed her personally identifying information (PII), including her name and Social Security number, to unauthorized third parties as a result of targeted data hack against her former employer was a concrete injury, as required for former employee to have Article III standing to bring negligence, breach of implied contract, and breach of confidence claims against her former employer and its parent; these concrete harms foreseeably arose from the exposure of former employee's PII to a malign outside actor, giving rise to a material risk of future harm. U.S. Const. art. 3, § 2, cl. 1.

More cases on this issue

[9] **Labor and Employment** Parties in general; standing

Former employee's allegations that the personally identifying information (PII) she entrusted to her former employer was exposed as a result of a targeted attempt by a third party to access the data set, in which a hacker leveraged a vulnerability in a third party's software and gained access to her PII, and that the PII taken by the hackers included her name and Social Security number (SSN), the kind of information

that gave rise to a high risk of identity theft, were sufficient to suggest a substantial likelihood of future harm, satisfying the actual or imminent harm component of the injury in fact element of Article III standing to sue former employer and its parent, even though employee did not allege any known misuse of information in the dataset accessed in the hack. U.S. Const. art. 3, § 2, cl. 1.

1 Case that cites this headnote
More cases on this issue

[10] **Labor and Employment** Parties in general; standing

Was injury in fact requirement for standing satisfied?**Yes**

Former employee's allegation that her specific personally identifying information (PII) was compromised during a targeted data hack of her former employer sufficiently alleged an injury distinct from the body politic, and thus satisfied the particularity component of the injury in fact element of Article III standing to sue former employer and its parent. U.S. Const. art. 3, § 2, cl. 1.

More cases on this issue

[11] **Telecommunications** Data breaches; hacking

Torts Miscellaneous torts in general

Former employee pled cognizable damages with reasonable certainty, as required to state claims against former employer and its parent for negligence, breach of implied contract, and breach of confidence arising from the exposure of the personally identifying information (PII), including her name and Social Security number, as a result of a targeted data hack of the information she had entrusted to employer; employee alleged the risk of future harm due to the exposure of her private information to an unauthorized malevolent actor, and that she had spent time and money trying to mitigate the consequences of the data breach through the prevention, detection, and recovery from identity theft.

More cases on this issue

[12] **Federal Courts** Parties, process, and notice

Former employee did not waive her challenge to district court's dismissal, for failure to state a claim, of her claims for damages against her former employer and its parent arising from the exposure of her personally identifying information (PII) as a result of a targeted data hack; district court's conclusion that former employee did not plausibly plead damages rested entirely on the court's conclusion that she lacked Article III standing to seek damages based upon a risk of future harm, and employee's challenge to that conclusion was a challenge to the court's analysis of her damages. U.S. Const. art. 3, § 2, cl. 1; Fed. R. Civ. P. 12(b)(6).

More cases on this issue

[13] **Damages** Nature and theory of compensation

Federal Civil Procedure In general; injury or interest

To say that the plaintiffs have Article III standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available. U.S. Const. art. 3, § 2, cl. 1.

***279** Appeal from the United States District Court for the Southern District of New York (Hellerstein, *J.*)

Attorneys and Law Firms

John A. Yanchunis, Kenya Reddy, Morgan and Morgan, Tampa, FL, for Plaintiff-Appellant.

Travis LeBlanc, Cooley LLP, Washington, D.C., Tiana Demas, Cooley LLP, New York, NY, for Defendants-Appellees.

Before: Newman, Nardini, and Robinson, Circuit Judges.

Opinion

Robinson, Circuit Judge:

This case requires us to consider the proper framework for evaluating whether an individual whose personally identifying information ("PII") is exposed to unauthorized actors, but has not (yet) been used for injurious purposes such as identity theft, has suffered an injury in fact for purposes of (1) Article III standing to sue for damages and (2) pleading a "claim upon which relief can be granted," Fed. R. Civ. P. 12(b)(6). In particular, we are called upon to determine how the Supreme Court's decision in *TransUnion, LLC v. Ramirez*, —— U.S. ——, 141 S. Ct. 2190, 210 L.Ed.2d 568 (2021), impacts this Court's previous holding in *McMorris v. Carlos Lopez & Associates*, 995 F.3d 295, 303 (2d Cir. 2021).

[1] **[2]** To establish Article III standing under the U.S. Constitution, a plaintiff must show (1) an injury in fact (2) caused by the defendant, (3) that would likely be ***280** redressable by the court. *Thole v. U.S. Bank N.A.*, —— U.S. ——, 140 S. Ct. 1615, 1618, 207 L.Ed.2d 85 (2020). At issue here is the first element: injury in fact. "Injury in fact," in turn, embodies three components: it must be "concrete, particularized, and actual or imminent." *Id.* We conclude that with respect to the question whether an injury arising from risk of future harm is sufficiently "concrete" to constitute an injury in fact, *TransUnion* controls; with respect to the question whether the asserted injury is "actual or imminent," the *McMorris* framework continues to apply in data breach cases like this.

[3] Plaintiff-Appellant Nancy Bohnak appeals from an order [1] of the United States District Court for the Southern District of New York (Hellerstein, *J.*) dismissing her claims against Defendants-Appellees Marsh & McLennan Agency, LLC ("MMA") and Marsh & McLennan Companies ("MMC") (together, "Defendants") for failure to state a claim. [2] *Bohnak v. Marsh & McLennan Cos., Inc.*, 580 F. Supp. 3d 21 (S.D.N.Y. 2022). Applying the above framework, we conclude that Bohnak's allegation that an unauthorized third party accessed her name and Social Security number ("SSN") through a targeted data breach gives her Article III standing to bring this action against the defendants to whom she had entrusted her PII. We further conclude that the district court erred in dismissing Bohnak's claims for failure to plausibly allege cognizable damages because we hold that by pleading a sufficient Article III injury in fact, Bohnak also satisfies the damages element of a valid claim for relief.

For the reasons set forth below, we REVERSE the district court's order dismissing Bohnak's claims for damages and REMAND for further proceedings.

BACKGROUND [3]

MMC "is the world's leading professional services firm in the areas of risk, strategy and people," App'x 9, ¶ 3; MMA is a wholly owned subsidiary of MMC and serves "the risk prevention and insurance needs of middle market companies in the United States," *id.* ¶ 4. Defendants stored PII such as "Social Security or other federal tax identification number[s], driver's license or other government issued identification, and passport information" of at least 7,000 individuals. App'x 8-9, ¶ 2. The PII at issue relates to "(i) Defendants' current and former employees and spouses and dependents thereof; (ii) current and former employees of Defendants' clients, contractors, applicants and investors; and (iii) individuals whose information Defendants acquired through the purchase of or ***281** merger with another business." App'x 8, ¶ 1.

Bohnak is MMA's former employee, and "[a]s a condition of [ ] Bohnak's employment, Defendants required that she entrust her PII, including but not limited to her Social Security or other federal tax id number." [4] App'x 21, ¶ 58.

In April 2021 an "unauthorized actor ... leveraged a vulnerability in a third party's software" and accessed Bohnak's PII, including her "name and ... Social Security or other federal tax id number." App'x 14, ¶ 30.

PII is of "high value to criminals, as evidenced by the prices they will pay through the dark web." [5] App'x 17, ¶ 44. "[SSNs], for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change." App'x 18, ¶ 45. Specifically, "[a]n individual cannot obtain a new [SSN] without significant paperwork and evidence of actual misuse." *Id.* ¶ 46.

Despite the sensitivity of the data in Defendants' possession, they did not secure the data from potential unauthorized actors through encryption, and the data continues to be unencrypted.

In contrast, Bohnak has been "very careful about sharing her PII. She has never knowingly transmitted her unencrypted

sensitive PII over the internet or any other unsecured source." App'x 21, ¶ 61. She "stores any documents containing her PII in a safe and secure location or destroys the documents," and "she diligently chooses unique usernames and passwords for her various online accounts." App'x 21–22, ¶ 62.

After Defendants notified Bohnak of the data breach (two months after Defendants learned of the incident), Bohnak filed this nationwide class action on behalf of herself and others similarly situated. She alleges that Defendants failed to: "(i) adequately protect the PII of [Bohnak] and Class Members; (ii) warn [Bohnak] and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents." App'x 11, ¶ 14.

Asserting state law claims of negligence, breach of implied contract, and breach of confidence, Bohnak alleges that she and Class Members suffered the following injuries:

> (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession ***282** and is subject to further unauthorized disclosures so long as Defendants fail[ ] to undertake appropriate and adequate measures to protect the PII.

App'x 11, ¶ 15.

Defendants moved to dismiss Bohnak's complaint under Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction, arguing that Bohnak lacks Article III standing. In the alternative, Defendants moved to dismiss the complaint under Rule 12(b)(6) because Bohnak fails to allege any cognizable damages.

The district court rejected Defendants' argument that Bohnak lacked Article III standing, reasoning that, although the future, indefinite risk of identity theft involving her compromised PII by itself was insufficient to establish an injury in fact under *TransUnion*, Bohnak plausibly alleged a separate concrete injury, analogous to that associated with the common-law tort of public disclosure of private information, that could support Article III standing.

However, the district court accepted Defendants' argument that Bohnak had failed to state a claim for which relief can be granted, reasoning that she had not plausibly alleged cognizable damages arising from the disclosure of her PII. In particular, the district court concluded that Bohnak could only speculate about the extent of any future harm, and that the damages arising from any risk of future harm are not "capable of proof with reasonable certainty." *Bohnak,* 580 F. Supp. 3d at 31. The court concluded that Bohnak's alleged loss of time and money responding to the increased risk of harm is not "cognizable" because it was not proximately caused by the harm of disclosure which, the court emphasized, was "the only harm for which [the court] found Plaintiffs have Article III standing." *Id.*

Moreover, the court reasoned that Bohnak's prayer for injunctive relief is based on the same harms as her claims for monetary relief, indicating the harms are compensable through money damages. In the court's view, a permanent injunction is thus unavailable. Because the court concluded that Bohnak does not plausibly allege a claim for damages or injunctive relief, it dismissed Bohnak's claims pursuant to Rule 12(b)(6). Bohnak appealed.

DISCUSSION

Bohnak challenges the district court's conclusion that she cannot establish standing merely by virtue of the risk of future misuse of her PII (such as identity theft or fraud), and in so arguing implicitly challenges the reasoning underlying the court's dismissal of her claims for failure to state a cognizable claim for damages. Defendants, on the other hand, contend that because her claims are predicated on a risk of future harm, Bohnak lacks standing altogether.

We conclude that Bohnak has standing to pursue her claims for relief, and that she has adequately alleged a cognizable claim for damages. [6]

I. Standing

We first consider whether Bohnak has established Article III standing. *See* ***283** *Central States SE and SW Areas Health and Welfare Fund v. Merck–Medco Managed Care, LLC*, 433 F.3d 181, 198 (2d Cir. 2005) ("If plaintiffs lack Article III standing, a court has no subject matter jurisdiction to hear their claim.").

[4] **[5]** "Because standing is challenged on the basis of the pleadings, we accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party." *W.R. Huff Asset Mgmt. Co., LLC v. Deloitte & Touche, LLP*, 549 F.3d 100, 106 (2d Cir. 2008) (internal quotation marks omitted). In this context, we determine whether a plaintiff has constitutional standing to sue without deference to the district court. *Id.*

As noted above, to establish Article III standing, a plaintiff must show (1) an injury in fact that is "concrete, particularized, and actual or imminent," (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressable by the court. *Thole*, 140 S. Ct. at 1618. At issue here is the first element—an injury in fact that is "concrete, particularized, and actual or imminent."

Bohnak argues that the district court erred by concluding that the risk of future harm arising from the disclosure of her PII is not a cognizable injury for standing purposes. In particular, she argues that the district court erred in concluding that the Supreme Court's decision in *TransUnion* calls into question the continuing vitality of this Court's decision in *McMorris*. And she contends that under the framework established in *McMorris*, she has standing to pursue her claims.

Defendants contend that *TransUnion* forecloses any argument that Bohnak has standing based on a risk of future harm, that Bohnak cannot establish standing based on the factors set forth in *McMorris*, and that the district court erred in concluding that Bohnak did have standing to pursue her claims based on the injury from the exposure of her PII.

We conclude that *TransUnion* is the touchstone for determining whether Bohnak has alleged a concrete injury, and that under *TransUnion*, Bohnak's alleged injuries arising from the risk of future harm are concrete. We further conclude that *McMorris* is the touchstone for determining whether Bohnak has alleged an "actual or imminent" injury, and that under *McMorris*, Bohnak's alleged injuries are "actual or imminent." *McMorris*, 995 F.3d at 300. Given these conclusions, and because the other elements of Article III standing are undisputedly met, we conclude that Bohnak has Article III standing, and we have jurisdiction to review this appeal.

A. TransUnion: Concreteness

i. The Court's Holding

In *TransUnion*, in a distinct but somewhat analogous context, the Supreme Court considered whether a risk of future injury alone is sufficiently concrete to be an injury in fact for purposes of Article III standing. 141 S. Ct. at 2204 ("The question in this case focuses on the Article III requirement that the plaintiff's injury in fact be 'concrete,'—that is, 'real, and not abstract.' ").

The conflict in *TransUnion* arose from a product designed to help businesses avoid transacting with individuals on the United States Treasury Department's Office of Foreign Assets Control ("OFAC") list of "specially designated nationals who threaten America's national security." *Id.* at 2201-02 (internal quotation marks omitted). When TransUnion (a "Big Three" credit reporting agency) conducted a credit check for subscribers to their special service, it used third-party software to compare the consumer's name against the ***284** OFAC list. *Id.* at 2201. As the Supreme Court explained,

> If the consumer's first and last name matched the first and last name of an individual on OFAC's list, then TransUnion would place an alert on the credit report indicating that the consumer's name was a "potential match" to a name on the OFAC list. TransUnion did not compare any data other than first and last names.

Id.

TransUnion's system produced many false positives, as many law-abiding Americans share names with individuals on OFAC's list of specially designated nationals. *Id.* Sergio Ramirez, the named plaintiff, was one such law-abiding American. *Id.* He tried to purchase a car from a dealership, but the dealership refused to sell it to him after receiving a report from TransUnion that he was on OFAC's list. *Id.* Ramirez filed a class action on behalf of himself and the rest of the proposed 8,185 class members seeking statutory damages for TransUnion's violations of the Fair Credit Reporting Act ("FCRA" or the "Act"). *Id.* at 2200. FCRA "imposes a host of requirements concerning the creation and use of consumer reports." *Id.* (internal quotation marks omitted). Ramirez alleged that in connection with its new product, TransUnion "failed to follow reasonable procedures to ensure the accuracy of information in his credit file." *Id.* at 2202. The proposed class of individuals all received notice from TransUnion that their names were considered a potential match to names on the OFAC list. *Id.* During the class period, TransUnion had distributed reports to potential creditors concerning only 1,853 of the 8,185 class members. *Id.*

In evaluating whether all of the class members' injuries arising from TransUnion's alleged statutory violations had suffered an injury in fact supporting Article III standing, the Supreme Court focused its analysis on the issue of whether the plaintiffs had shown a "concrete harm." *Id.* at 2208–09.

In considering whether the plaintiffs' alleged injuries were sufficiently concrete to constitute an injury in fact for purposes of their claim for damages, the Court considered whether their injuries bore a " 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 2204 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341, 136 S.Ct. 1540, 194 L.Ed.2d 635 (2016)). The Court recognized that "traditional tangible harms," such as physical harms and monetary harms, "readily qualify as concrete injuries under Article III." *Id.* But it went on to recognize that harms beyond those traditional tangible harms can also support standing:

> Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion.

Id. (citation omitted).

Applying this framework, the Court had "no trouble" concluding that the 1,853 class members whose false OFAC designations were sent to third parties had suffered a concrete injury. *Id.* at 2209. The Court reasoned that such an injury "bears a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—namely, the reputational harm associated with the tort of defamation." *Id.* (quoting *Spokeo*, 578 U.S. at 341, 136 S.Ct. 1540). Therefore, the Court concluded that the 1,853 class members whose reports were disseminated to third parties suffered a concrete injury in fact under Article III. *Id.* Significantly, the ***285** Court concluded that the publication of false information about these class members to third parties was itself enough to establish a concrete injury; it did not take further steps to evaluate whether those third parties *used* the information in ways that harmed the class members. *Id.*

On the other hand, the Court concluded that the remaining 6,332 class members whose credit reports were not shared with third parties had not suffered a concrete injury, explaining that there is "no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury." *Id.* (internal quotation marks omitted). The Court distinguished between credit reports published to third parties and files that consumer reporting agencies maintain internally. *Id.* at 2210. It analogized misleading information merely sitting in a company database to a defamatory letter stored in a desk drawer and never sent; the Court explained that in both cases, legally speaking, nobody is harmed. *Id.*

The Court gave two answers of note in response to the arguments on behalf of the 6,332 class members that the existence of misleading OFAC alerts in their internal credit files exposed them to a material risk that the information would be disseminated to third parties *in the future* and thereby caused them present harm.

First, it explained that, although mere risk of future harm does not provide standing to seek retrospective damages where actual harm never materialized, "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk

of harm is sufficiently imminent and substantial." *Id.* (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5, 133 S.Ct. 1138, 185 L.Ed.2d 264 (2013)).

Second, the Court noted that a risk of future harm could "itself cause[ ] a *separate* concrete harm," in which case the plaintiff would have standing to pursue damages premised on that separate concrete harm. *Id.* at 2211 (emphasis in original). For example, the Court suggested that evidence that the class members suffered some other injury, such as emotional injury, from the risk that their reports would be provided to third-party businesses could give them standing to seek damages. *Id.*

These principles guide our assessment of whether Bohnak's alleged harm is sufficiently "concrete" to support Article III standing.

ii. Application to Bohnak's Claims

[6] Like the Supreme Court in *TransUnion*, we have no trouble concluding that Bohnak's alleged harm is sufficiently concrete to support her claims for damages. Similar to the publication of misleading information about some of the plaintiffs in *TransUnion*, the core injury here—exposure of Bohnak's private PII to unauthorized third parties—bears some relationship to a well-established common-law analog: public disclosure of private facts. *See Restatement (Second) Torts* § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of ... privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."). Bohnak's position is thus similar to that of the 1,853 class members who had standing in *TransUnion* based on the publication of misleading information to third parties without regard to whether the third parties used the information to cause additional harm.

***286** We need not stretch to reach this conclusion. In *TransUnion* itself, the Supreme Court specifically recognized that "disclosure of private information" was an intangible harm "traditionally recognized as providing a basis for lawsuits in American courts." 141 S. Ct. at 2204 (citing *Davis v. Federal Election Comm'n*, 554 U.S. 724, 733, 128 S.Ct. 2759, 171 L.Ed.2d 737 (2008)). It thus described an injury arising from such disclosure as "concrete" for purposes of the Article III analysis. *Id.* The core of the injury Bohnak alleges here is that she has been harmed by the exposure of her private information—including her SSN and other PII—to an unauthorized malevolent actor. This falls squarely within the scope of an intangible harm the Supreme Court has recognized as "concrete." *Id.*

[7] We recognize that Bohnak does not in this case assert a common law claim for public disclosure of private facts, and it matters not whether New York common law recognizes a tort relating to publication of private facts. For the purposes of the "concreteness" analysis under *TransUnion*, what matters is that the intangible harm arising from disclosure of one's PII bears a relationship to an injury with a "close historical or common-law analogue." *Id.* And that analog need not be "an exact duplicate." *Id.* at 2209.

[8] In addition, Bohnak's allegations establish a concrete injury for purposes of her damages claim for a separate reason: she has suffered "separate concrete harm[s]" as a result of the risk of future harm occasioned by the exposure of her PII. *Id.* at 2211 (emphasis omitted). In particular, she has alleged among other things that she incurred "out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft" and "lost time" and other "opportunity costs" associated with attempting to mitigate the consequences of the data breach. App'x 11, ¶ 15. These separate and concrete harms foreseeably arising from the exposure of Bohnak's PII to a malign outside actor, giving rise to a material risk of future harm, independently support standing.

Our conclusion on this point is consistent with our analysis in *McMorris*, in which we explained with reference to the injury-in-fact question more broadly that "where plaintiffs have shown a substantial risk of future identity theft or fraud, any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact." 995 F.3d at 303 (internal quotation marks omitted).

It also echoes the First Circuit's conclusion in *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365 (1st Cir. 2023). In that case, the First Circuit considered the standing of a plaintiff whose PII had been exposed in a data breach by a home-delivery pharmacy service. There was no allegation that the plaintiff's PII had actually been misused, although other PII in the same dataset had been. Applying the lessons of *TransUnion*, the court concluded that the plaintiff had plausibly alleged a "separate concrete, present harm" caused by exposure to the risk of future harm. *Webb*, 72 F.4th at

376. In particular, the plaintiff had alleged that she spent "considerable time and effort" monitoring her accounts to protect them. *Id.* (internal quotation marks omitted). The First Circuit joined 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." *Id.* at 377. The court noted, "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 ***287** incurring costs in anticipation of non-imminent harm.' " *Id.* (quoting *Clapper*, 568 U.S. at 422, 133 S.Ct. 1138).

The Third Circuit reached a similar conclusion in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022)—another post-*TransUnion* data breach case. In *Clemens*, the Third Circuit concluded:

> Following *TransUnion's* guidance, we hold that in the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as [the plaintiff] alleges that the exposure to that substantial risk caused additional, currently felt concrete harms. For example, if the plaintiff's knowledge of the substantial risk of identity theft causes [the plaintiff] to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury.

Id. at 155–56; *see also In re U.S. OPM Data Security Breach Litigation*, 928 F.3d 42, 59 (D.C. Cir. 2019) (noting that the Supreme Court has recognized standing to sue "on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists" (quoting discussion of *Clapper* in *Hutton v. Nat'l Bd. of Examiners in Optometry*, 892 F.3d 613, 622 (4th Cir. 2018))); *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829-30 (7th Cir. 2018) (monthly fees for credit monitoring secured in response to a data breach are "real and measurable" actual damages).

For these reasons, given the close relationship between Bohnak's data exposure injury and the common law analog of public disclosure of private facts, and, alternatively, based on her allegations that she suffered concrete present harms due to the increased risk that she will in the future fall victim to identity theft as a result of the data breach, we conclude that Bohnak has alleged an injury that is sufficiently concrete to constitute an injury in fact for purposes of her damages claim.

B. McMorris: Imminence

Our conclusion that Bohnak's injury is concrete does not fully resolve the standing question because it addresses only one component of injury in fact. The "particularity" requirement for an injury in fact is not in dispute here, but whether Bohnak's injury is "actual or imminent" is. Our pre-*TransUnion* decision in *McMorris* guides our analysis of this component.

i. The Court's Holding

In *McMorris*, the plaintiffs brought a putative class action against their employer asserting claims for negligence and violations of consumer protection laws resulting from inadvertent dissemination of a company-wide email containing their sensitive PII. 995 F.3d at 298. The plaintiffs alleged that because their PII had been disclosed to all of the defendant's then current employees, plaintiffs were "at imminent risk of suffering identity theft and becoming the victims of unknown but certainly impending future crimes." *Id.* (internal quotation marks omitted).

As in this case, the issue in *McMorris* was whether the plaintiffs had suffered an injury in fact. 995 F.3d at 300. But, in *McMorris* we considered the question holistically, without breaking the injury-in-fact analysis into its components. *See id.* ("This case concerns ... the first element of Article III standing: the existence of an injury in fact."). Because many of our insights in *McMorris* relate most closely to the issue of whether the future harm is sufficiently "actual or imminent," *TransUnion*, which did not purport to address ***288** matters beyond "concreteness," does not fully supplant our analysis in *McMorris*.

In *McMorris*, we explained that "a future injury constitutes an Article III injury in fact only 'if the threatened injury is certainly impending, or there is a substantial risk that the harm

will occur.' " 995 F.3d at 300 (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158, 134 S.Ct. 2334, 189 L.Ed.2d 246 (2014)). We then identified and endorsed three non-exhaustive factors that courts have considered in determining whether plaintiffs whose PII has been compromised but not yet misused face a substantial risk of harm.

First, we said that the most important factor in determining whether a plaintiff whose PII has been exposed has alleged an injury in fact is whether the data was compromised as the result of a targeted attack intended to get PII. *McMorris*, 995 F.3d at 301. Where a malicious third party has intentionally targeted a defendant's system and has stolen a plaintiff's data stored on that system, courts are more willing to find a likelihood of future identity theft or fraud sufficient to confer standing. *Id.* We embraced the Seventh Circuit's reasoning in one such case: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)).

Second, we observed that, "while not a necessary component of establishing standing," courts have been more likely to conclude that a plaintiff has established a "substantial risk of future injury" where some part of the compromised dataset has been misused—even if a plaintiff's own data has not. *Id.* at 301. For example, fraudulent charges to the credit cards of *other* customers impacted by the same data breach, or evidence that a plaintiff's PII is available for sale on the Dark Web, can support a finding that a plaintiff is at a substantial risk of identity theft or fraud. *Id.* at 301–02.

Third, we explained that courts may consider whether the exposed PII is of the type "more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed." *Id.* at 302. On one hand, we noted that "the dissemination of high-risk information such as [SSNs] ... especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud." *Id.* On the other hand, we reasoned that the exposure of data that is publicly available, or that can be rendered useless (like a credit card number unaccompanied by other PII), is less likely to subject plaintiffs to a perpetual risk of identity theft. *Id.*

Insofar as these factors shed light on whether the future harm of identity theft or fraud resulting from a data breach is sufficiently actual and imminent (as opposed to concrete), we see nothing in *TransUnion* that overrides our analysis, and *McMorris* remains a touchstone.

ii. Application to Bohnak's Claims

[9] Considering these three factors, we conclude that Bohnak has sufficiently alleged that she faces an imminent risk of injury—that is, a "substantial risk that the harm will occur." *Id.* at 300 (internal quotation marks omitted).

First and foremost, Bohnak has alleged that her PII was exposed as a result of a targeted attempt by a third party to access the data set. App'x 14, ¶ 30; *see McMorris*, 995 F.3d at 301 (considering "whether the data at issue has been compromised as the ***289** result of a targeted attack intended to obtain the plaintiffs' data."). In particular, she alleges, based on Defendants' own report to her, that an "unauthorized actor [i.e., a hacker] ... leveraged a vulnerability in a third party's software" and gained access to her PII. App'x 14, ¶ 30. This was not an inadvertent, intra-company disclosure; it was a targeted hack.

Second, Bohnak alleges that the PII taken by the hackers includes her name and SSN. *Id.* This is exactly the kind of information that gives rise to a high risk of identity theft. *McMorris*, 995 F.3d at 302. As Bohnak has alleged, SSNs "are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change." App'x 18, ¶ 45. And one cannot get a new SSN without "evidence of actual misuse," making it difficult to take preventive action to guard against the misuse of the compromised number. *Id.* ¶ 46.

We recognize that Bohnak has not pulled off a hat trick with respect to the factors identified in *McMorris*; she has not alleged any known misuse of information in the dataset accessed in the hack. But we emphasized in *McMorris* that such an allegation is not necessary to establish that an injury is sufficiently imminent to constitute an injury in fact. 995 F.3d at 301. We conclude that the allegations of a targeted hack that exposed Bohnak's name and SSN to an unauthorized actor are sufficient to suggest a substantial likelihood of future harm, satisfying the "actual or imminent harm" component of an injury in fact.

[10] Because Bohnak has alleged a concrete and imminent injury, and because her injury is undisputedly particular, she

has pled an injury in fact.[7] And because Bohnak has pled that Defendants caused her injury, and her injuries would be redressed through money damages, we conclude that Bohnak has Article III standing to pursue her damages claim.[8]

II. Bohnak's Damages Claim

[11] **[12]** Our discussion of standing all but disposes of the damages issue.[9] The district court dismissed Bohnak's claims on the basis that her damages are not "capable of proof with reasonable certainty," and her alleged loss of time and money responding to the increased risk of harm was not "cognizable." *Bohnak*, 580 F. Supp. 3d at 31.

[13] For the reasons set forth above, Bohnak's alleged injury arising from the increased risk of harm *is* cognizable for standing purposes, and thus could support ***290** a claim for damages. As the Seventh Circuit explained in a similar case: "To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available." *Dieffenbach*, 887 F.3d at 828.

Moreover, Bohnak has pled additional injuries—the time and money spent trying to mitigate the consequences of the data breach—with respect to which damages are unquestionably capable of reasonable proof. *See* App'x 11 ¶ 15; *see E.J. Brooks Co. v. Cambridge Sec. Seals,* 31 N.Y.3d 441, 448–49, 105 N.E.3d 301 (2018) (compensatory damages "cannot be remote, contingent or speculative," but the standard "is not one of 'mathematical certainty' but only 'reasonable certainty' " (quoting *Steitz v. Gifford*, 280 N.Y. 15, 20, 19 N.E.2d 661 (1939))); *Aqua Dredge, Inc. v. Stony Point Marina & Yacht Club, Inc.*, 183 A.D.2d 1055, 583 N.Y.S.2d 648, 650 (3d Dep't 1992) ("In computing damages for breach of contract, mathematical certainty is rarely attained or even expected.").

CONCLUSION

In sum, we conclude that the Supreme Court's decision in *TransUnion* governs the analysis of whether a risk of future injury is sufficiently concrete to constitute an injury in fact for purposes of a claim for damages and that our analysis in *McMorris* continues to guide our assessment of the "imminence" component of injury in fact for purposes of Article III standing. Applying these cases, we hold that Bohnak has Article III standing to bring her claims for damages and that the district court erred in dismissing her claims for failure to plead cognizable damages with reasonable certainty.

For these reasons, we REVERSE the district court's judgment dismissing Bohnak's claims for damages and REMAND for further proceedings consistent with this opinion.

All Citations

79 F.4th 276

Footnotes

1 The notice of appeal states that Bohnak appeals "from the Order and Opinion ... entered ... on January 17, 2022." (The order was in fact entered January 18, 2022, *see* Dist. Ct. Dkt. No. 32.) That order is appealable because it was a "final decision," 28 U.S.C. § 1291, that disposed of the entire case, *see Bankers Trust Co. v. Mallis*, 435 U.S. 381, 387, 98 S.Ct. 1117, 55 L.Ed.2d 357 (1978) ("[T]he District Court clearly evidenced its intent that the opinion and order from which an appeal was taken would represent the final decision in the case."). However, when a judgment is entered, as it was in this case on January 28, 2023 (Dist. Ct. Dkt. No. 33), the better practice is to appeal the judgment. That avoids any dispute as to whether an earlier entered order qualifies as a final decision.

2 Janet Lee Smith was a plaintiff in the underlying action but is not a party to this appeal.

3 This account is drawn from the allegations in Bohnak's complaint, which we must accept as true for purposes of evaluating Defendants' motion to dismiss. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009).

4 The record is silent as to when Bohnak's employment with MMA began, but it ended "[i]n or around 2014." App'x 21 ¶ 58.

5 "The Dark Web is a general term that describes hidden Internet sites that users cannot access without using special software." *McMorris*, 995 F.3d at 302 n.4 (quoting Kristin Finklea, Cong. Rsch. Serv., 7-5700, *Dark Web* 2 (2017)). "Not surprisingly, criminals and other malicious actors ... use the [D]ark [W]eb to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft." *Id.* (quoting Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1090 (2017)).

6 Bohnak has not challenged the district court's determination that she failed to plausibly allege a claim that would entitle her to injunctive relief, and her challenge to the district court's standing analysis does not directly undercut the court's rationale for dismissing her claims for injunctive relief. Accordingly, we deem any challenge to the district court's dismissal of her claim for injunctive relief waived, and do not address her claims for injunctive relief on appeal.

7 No party has suggested that the "particularity" requirement for an injury in fact is an obstacle to Bohnak's claims. *See Strubel v. Comenity Bank*, 842 F.3d 181, 188 (2d Cir. 2016) (explaining that "to satisfy the particularity requirement" an injury must be "distinct from the body politic"). Here, Bohnak has specifically alleged that *her* PII was compromised during a data breach that impacted a finite number of people, making her injury "distinct from the body politic."

8 Defendants challenge Bohnak's claims on the merits on the basis that she hasn't plausibly alleged cognizable damages. But in contesting her standing, Defendants have not argued that Bohnak has failed to establish the causation and redressability elements of standing.

9 We reject Defendants' contention that Bohnak waived her challenge to the district court's dismissal of her claim pursuant to Rule 12(b)(6). In this case, the district court's conclusion that Bohnak did not plausibly plead damages rested entirely on the court's conclusion that she lacked standing to seek damages based upon a risk of future harm. Bohnak's challenge to that conclusion *was* a challenge to the court's analysis of her damages.

End of Document