IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

SCOTT JENKINS, individually and on behalf of all others similarly situated, **Plaintiff**, **v.** **ASSOCIATED WHOLESALE GROCERS, INC.,** **Defendant**.	**Case No. 24-4039-DDC-GEB**

MEMORANDUM AND ORDER

Plaintiff Scott Jenkins alleges unauthorized third parties accessed his personal identifying information (PII) in a data breach. According to him, defendant Associated Wholesale Grocers didn't maintain secure data systems. Plaintiff asserts a number of claims, on behalf of himself and a prospective class. Defendants moved to dismiss under Fed. R. Civ. P. 12(b)(1)—arguing plaintiff lacks standing. They also invoke Rule 12(b)(6)—arguing plaintiff has failed to state a claim. *See* Doc. 18 at 1.

Article III standing is complicated in data breach cases. The analyses of courts across the country reflect as much—revealing differing results turning on nuanced facts. The court addresses plaintiff's alleged injuries in the context of the varied authority. The court concludes plaintiff lacks standing to seek monetary, injunctive, and declaratory relief—at least on the allegations in the Complaint (Doc. 1). With that conclusion comes another: the court doesn't

have jurisdiction over this dispute. So, the court must dismiss plaintiff's Complaint.[1] Below, the court explains these decisions, beginning with a brief background.

I. Background

The following facts are taken from allegations in plaintiff's Complaint.

The PII

Plaintiff is defendant's former employee. Doc. 1 at 3 (Compl. ¶ 13). As part of the hiring process, defendant required plaintiff to provide certain PII. *Id.* at 4 (Compl. ¶ 21). And plaintiff relied on defendant to maintain confidentially and secure his PII for business purposes. *Id.* (Compl. ¶ 22). Plaintiff, for his part, is careful to avoid sharing his PII. *Id.* at 15 (Compl. ¶ 72). He stores sensitive documents in secure locations or destroys them. *Id.* (Compl. ¶ 73). His usernames and passwords are unique. *Id.*

All this focus on security matters, plaintiff contends, because PII is highly valuable to criminal actors. *Id.* at 12 (Compl. ¶ 57). Unauthorized actors sell PII on the Dark Web, use PII to apply for government benefits or medical services, and cross-reference PII with other data to develop detailed dossiers—known as "Fullz packages"—about individuals. *Id.* at 12–14 (Compl. ¶¶ 58–63).

The Breach

In October 2023, an unknown actor breached defendant's computer systems. *Id.* at 1 (Compl. ¶ 1). The breach released the PII of plaintiff (and a putative class). *Id.* Included in the breach were plaintiff's name, Social Security number, and date of birth. *Id.* at 14 (Compl. ¶ 66). But it wasn't until April 2024 that defendant notified plaintiff about the breach. *Id.* at 5 (Compl. ¶ 26). And when defendant did so, it left some details to the imagination. Defendant didn't

[1] Because of the court's standing decision, this Order doesn't address defendant's 12(b)(6) motion.

explain the breach's "root cause[,]" "vulnerabilities exploited," or "remedial measures" taken to prevent a future data breach. *Id.* (Compl. ¶ 28).

Plaintiff asserts defendant's security procedures weren't appropriate. *Id.* (Compl. ¶ 30). That's because defendant stored plaintiff's PII in an unencrypted, Internet-accessible environment. *Id.* at 7 (Compl. ¶ 37). And plaintiff outlines a host of preventative measures defendant could have deployed. *Id.* at 8–11 (Compl. ¶¶ 45–47).

The Aftermath

After the data breach occurred, plaintiff has faced ongoing worry about when and how unauthorized actors may use his sensitive information. *Id.* at 15 (Compl. ¶ 67). Such misuse has begun already, he alleges. For starters, plaintiff received multiple notifications about unauthorized purchases on his PayPal account and sign-in attempts to his bank accounts. *Id.* (Compl. ¶ 68). Cybercriminals "were able to pose as Plaintiff and hack his financial accounts to steal his money." *Id.* (Compl. ¶ 69). On top of that, plaintiff has received spam calls referencing falsified illegal actions. *Id.* (Compl. ¶ 70). These calls "are clearly attempts to use Plaintiff's PII to extort him for money or more PII." *Id.*

Plaintiff spent 240 hours cleaning up the data breach's consequences. *Id.* (Compl. ¶ 71) (describing time spent "verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts, reviewing credit reports, and mitigating fraud and identity theft). And plaintiff also experiences fear, anxiety, and increased concern for the loss of his privacy. *Id.* at 16 (Compl. ¶ 74).

Defendant still possesses plaintiff's PII. *Id.* at 32 (Compl. ¶ 155). Plaintiff believes defendant's security measures are still inadequate, though defendant "publicly denies these allegations." *Id.* at 38 (Compl. ¶ 189).

The Lawsuit

Plaintiff filed this lawsuit in May 2024, asserting claims of negligence, negligence per se, invasion of privacy, breach of implied contract, breach of confidence, and breach of fiduciary duty. *Id.* at 26–38 (Compl. ¶¶ 116–86). Plaintiff seeks monetary, injunctive, and declaratory relief. Doc. 1 at 38–39; 40–41 (Compl. ¶¶ 191–92; VII.2–3).

Defendant moved to dismiss the Complaint. Doc. 17. Plaintiff responded. Doc. 20. But, as defendant emphasizes, plaintiff filed his Response out of time. Doc. 21 at 1. Plaintiff's Response was due August 2, 2024. *See* Doc. 17 (filed July 12, 2024); *see also* D. Kan. Rule 6.1(d)(1) (requiring parties to file responses to dispositive motions within 21 days after service of the motion). Plaintiff didn't file his Response until August 6, 2024. Doc. 20. And a quick survey of the docket reveals that plaintiff never requested an extension of time. Defendant asks the court to sanction plaintiff by disregarding plaintiff's Response. Doc. 21 at 1.

The court has discretion to take such a course. *See Curran v. AMI Fireplace Co.*, 163 F. App'x 714, 718 (10th Cir. 2006) (concluding district court acted within its discretion in striking untimely response to summary judgment motion). But because the court concludes plaintiff's response doesn't change the outcome, the court declines to strike it. *See Sheldon v. Khanal*, No. 07-2112-KHV, 2008 WL 474262, at 2 n.3 (D. Kan. Feb. 19, 2008) ("Although the Court discourages such tardiness, it notes that these arguments will not materially change the resolution of plaintiffs' motion, and the Court therefore briefly considers the arguments.").

II. 12(b)(1) Legal Standard

Under Rule 12(b)(1), a defendant may move the court to dismiss for lack of subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). "Federal courts are courts of limited jurisdiction and, as such, must have a statutory basis to exercise jurisdiction." *Montoya v. Chao*, 296 F.3d

952, 955 (10th Cir. 2002). "A court lacking jurisdiction cannot render judgment but must dismiss the cause at any stage of the proceedings in which it becomes apparent that jurisdiction is lacking." *Basso v. Utah Power & Light Co.*, 495 F.2d 906, 909 (10th Cir. 1974). The party invoking federal jurisdiction bears the burden to prove it exists. *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994); *see also Siloam Springs Hotel, L.L.C. v. Century Sur. Co.*, 906 F.3d 926, 931 (10th Cir. 2018) (presuming "no jurisdiction exists absent an adequate showing by the party invoking federal jurisdiction").

Rule 12(b)(1) challenges fall into two categories: (1) facial attacks on allegations in the complaint to challenge their sufficiency and (2) factual attacks on the facts on which subject matter jurisdiction depends. *Holt v. United States*, 46 F.3d 1000, 1002–03 (10th Cir. 1995), *abrogated on other grounds by Cent. Green Co. v. United States*, 531 U.S. 425, 437 (2001); *Blood v. Labette Cnty. Med. Ctr.*, No. 22-cv-04036-HLT-KGG, 2022 WL 11745549, at *2 (D. Kan. Oct. 20, 2022) (explaining the two forms for a motion to dismiss for lack of jurisdiction under Rule 12(b)(1)). Facial attacks are resolved based solely on the complaint, accepting all the plaintiff's allegations as true. *Holt*, 46 F.3d at 1002.

Defendant here presents just a facial attack in its Motion to Dismiss. *See generally* Doc. 18. Accordingly, the court accepts plaintiff's allegations as true. *Holt*, 46 F.3d at 1002. But, on a standing challenge raised at the pleading stage, the "court need not accept 'conclusory allegations, unwarranted inferences, or legal conclusions.'" *Blood*, 2022 WL 11745549, at *3 (quoting *Brady Campaign to Prevent Gun Violence v. Brownback*, 110 F. Supp. 3d 1086, 1092 (D. Kan. 2015)); *Hackford v. Babbitt*, 14 F.3d 1457, 1465 (10th Cir. 1994) (same).

III. Standing

Article III of the United States Constitution limits federal courts' jurisdiction to "cases" and "controversies." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013). To present a case or controversy under Article III, a plaintiff must establish that he has standing to sue. *Id.* (citations omitted).

Article III's standing analysis requires three things: (1) an "injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical;" (2) "a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . traceable to the challenged action of the defendant, and not . . . the result of the independent action of some third party not before the court;" and (3) that it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992) (quotation cleaned up). At "the pleading stage, the plaintiff must clearly allege facts demonstrating each element" of standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citation, internal quotation marks, and ellipsis omitted). And, at the pleading stage, general factual allegations can carry plaintiff's burden to establish the elements of Article III standing because the court must "'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)). Plaintiff "must demonstrate standing for each claim that [he] press[es] and for each form of relief that [he] seek[s.]" *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021).

A. Standing Considerations in Data Privacy Cases

Data breach cases present unique Article III standing questions. The issues usually revolve around the first or second elements of standing: injury in fact and causation. One

problem in data breach cases is whether plaintiffs have suffered a *concrete* injury. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). "No concrete harm, no standing." *TransUnion*, 594 U.S. at 442.

Another problem is whether plaintiffs can *trace* their concrete injuries to the data breach alleged and in a nonspeculative manner. *See, e.g.*, *Blood*, 2022 WL 11745549, at *5 (emphasizing that plaintiffs must allege "a plausible, non-speculative connection from the stolen information" to the alleged injury to establish the causation element of standing). Traceability "requires a plaintiff to 'allege a substantial likelihood that the defendant's conduct caused [the] plaintiff's injury in fact.'" *Masterson v. IMA Fin. Grp.*, No. 23-2223-HTL-ADM, 2023 WL 8647157, at *3 (D. Kan. Dec. 14, 2023) (quoting *Santa Fe All. for Pub. Health & Safety v. City of Santa Fe*, 993 F.3d 802, 814 (10th Cir. 2021)).

Take the first problem—the injury in fact. Some Circuits have concluded that data breach plaintiffs have sustained injuries in fact because of the breach alone.[2] Others have

[2] *See, e.g.*, *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628–29 (D.C. Cir. 2017) (concluding plaintiffs had standing where plaintiffs alleged data breach exposed them to heightened risk of identity theft because "unauthorized party ha[d] already accessed personally identifying data on [defendant's] servers, and it [was] much less speculative—at the very least, it [was] plausible—to infer that this party ha[d] both the intent and the ability to use that data for ill" and focusing on the "light burden of proof the plaintiffs bear at the pleading stage"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 387–91 (6th Cir. 2016) (concluding plaintiffs had standing where hackers stole plaintiffs' personal information because where "data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes"); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 691–95 (7th Cir. 2015) (concluding plaintiffs had standing where hackers stole customer credit card numbers and explaining "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur" (quoting *Clapper*, 568 U.S. at 410)); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (concluding plaintiffs had standing where plaintiffs alleged concern about increased risk of future identity theft because plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1024–29 (9th Cir. 2018) (reaffirming *Krottner* post *Clapper*).

concluded the opposite.[3] Our Circuit has yet to weigh-in. But district courts across our Circuit have reached something of a consensus—injury in fact requires actual misuse of the PII. Merely experiencing a breach won't suffice.

The court has explained in an earlier decision that misuse of the compromised data is an important inflection point that explains many of the differing standing results. *C.C. v. Med-Data Inc.*, No. 21-2301-DDC-GEB, 2022 WL 970862, at *4 (D. Kan. Mar. 31, 2022) ("'[W]here no allegations of misuse are present, circuit courts have generally declined to find standing.'" (quoting *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 990 (W.D. Okla. 2021))); *In re Progressive Leasing Breach Litig.*, No. 23-cv-00783-DBB-CMR, 2025 WL 213744, at *9 (D. Utah Jan. 16, 2025) (cataloguing data privacy cases and concluding "misuse is generally necessary [for] standing").[4] Honing in on this inflection point, many district courts in the Tenth Circuit "have predicted that [our] Court of Appeals will require actual misuse of stolen data to

[3] *See O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023) ("[W]e've held that being subjected to a data breach isn't in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft."); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301, 303–05 (2d Cir. 2021) (noting "that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data" but ultimately concluding plaintiffs lacked standing because they "never alleged that their data was intentionally targeted or obtained by a third party," failed to allege their data "was in any way misused," and likewise failed to allege "that the PII was intentionally taken by an unauthorized third party or otherwise misused"); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340–44 (11th Cir. 2021) (concluding plaintiffs' alleged harms of substantial future risk of identity theft, proactive mitigation costs, and conclusory allegations of unauthorized charges failed to confer standing); *In re SuperValu, Inc.*, 870 F.3d 763, 769–70 (8th Cir. 2017) (concluding plaintiffs lacked standing when plaintiffs alleged that "illicit websites [were] selling their Card Information to counterfeiters and fraudsters, and that plaintiffs' financial institutions [were] attempting to mitigate their risk" because the allegations were "speculative" and "fail[ed] to allege any injury 'to the plaintiff[s]'" (quoting *Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000))).

[4] For a detailed assessment of cases addressing whether a plaintiff must allege actual misuse, see *In re Progressive*, 2025 WL 213744, at *3–9. A minority of courts have concluded a plaintiff has standing even absent allegations of actual misuse. *See Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 289 (2d Cir. 2023) (concluding plaintiff sufficiently alleged a substantial likelihood of future harm, even absent allegations of actual identity theft or other misuse).

find that plaintiffs have standing[.]" *Stern v. Academy Mortg. Corp.*, No. 24-cv-00015-DBB-DAO, 2025 WL 239036, at *3 (D. Utah Jan. 17, 2025); *Owen-Brooks v. DISH Network Corp.*, No. 23-cv-01168-RMR-SBP, 2024 WL 4338133, at *7–8 (D. Colo. Aug. 23, 2024), *report and recommendation adopted* 2024 WL 4333660 (D. Colo. Sept. 27, 2024) (joining sister courts "in predicting that the Tenth Circuit will *require* data breach plaintiffs to allege actual misuse of their stolen data . . . to find that they have standing to bring claims for *damages*. . . . [and] *injunctive relief*" (emphasis in original)); *cf. Blood*, 2022 WL 11745549, at *7 ("[M]ultiple Circuits have held that without actual misuse of stolen information, plaintiffs lack standing to bring claims because their injuries are not concrete, particularized, or imminent."). The court agrees with these sister courts—actual misuse generally is necessary to establish an injury in fact.

To put a finer point on it, actual misuse establishes a *past* harm—when a cybercriminal already has employed a plaintiff's PII for his own ends. But when it comes to PII, there's also the question of future harm—that is, if a plaintiff's PII is "out there," so to speak, a bad actor could use it at any point. The court addresses future harm separately, in a bit. It requires a slightly different analysis (one that includes, but doesn't end with actual misuse). For now, the court trains its attention on plaintiff's alleged harms to determine if any establish an injury in fact.

Plaintiff alleges four kinds of injury: (1) actual identity theft and the risk of future identity theft; (2) fear and anxiety; (3) lost time, annoyance, and inconvenience from mitigation efforts; and (4) loss of privacy. Doc. 1 at 15–16 (Compl. ¶¶ 68–75).[5] Each of these injuries

[5] Because a "'putative class action can proceed as long as one named plaintiff has standing[,]'" the court evaluates just the injury allegations specific to plaintiff. *Masterson*, 2023 WL 8647157, at *2 n.2 (quoting *In re SuperValu, Inc.*, 870 F.3d at 768).

allegedly supports a claim for damages. Plaintiff also requests declaratory and injunctive relief. Recall that plaintiff "must demonstrate standing for each claim that [he] press[es] *and* for each form of relief that [he] seek[s.]" *TransUnion*, 594 U.S. at 431 (emphasis added). To assess whether plaintiff has standing, the court evaluates each of his alleged injuries supporting damages. Then, the court addresses whether plaintiff has standing to seek injunctive and declaratory relief.

B. Damages

The court structures its standing analysis about damages as follows: *First*, the court evaluates plaintiff's alleged injuries premised on identity theft and fraud. These injuries subdivide into two categories—past and future identity theft. And each category merits a slightly different analysis. So, the court first addresses allegations of past identity theft, completing both the injury-in-fact and causation standing analyses. After completing that analysis, the court turns to future identity theft. It explains the three-part test employed when a court analyzes standing based on future identity theft allegations, and then conducts that analysis. As preview of the result, the court concludes that plaintiff doesn't have standing to seek damages premised on either past or future identity theft.

Then, the court assesses whether plaintiff has damages standing premised on emotional distress, lost time, or lost privacy injuries. Again, the answer is no for all three.

1. Past and Prospective Identity Theft and Fraud

Plaintiff alleges he "has had his identity stolen or attempts" at stealing his identity. Doc. 1 at 15 (Compl. ¶ 68). And he alleges that facing "imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse" of his data. *Id.* at 16 (Compl. ¶ 75). Start with plaintiff's alleged past identity theft.

a. Past Identity Theft

Three allegations of identity theft appear in plaintiff's Complaint. *First*, plaintiff alleges that because of the data breach, he received a number of spam calls. *Id.* at 15 (Compl. ¶ 70). Those calls, he asserts, were "clearly attempts to use Plaintiff's PII to extort him for money or more PII." *Id.* *Second*, he alleges unauthorized actors attempted to sign in to his bank accounts. *Id.* (Compl. ¶ 68). And, *third*, he alleges that cybercriminals "were able to pose as Plaintiff and hack his financial accounts to steal his money[,]" including making unauthorized purchases on his PayPal account. *Id.* (Compl. ¶¶ 68–69). The first and second of these allegations don't qualify as misuse constituting injuries in fact. The third *is* misuse constituting an injury in fact. But on that third allegation—as the court shows, below—plaintiff's standing theory runs out on causation.

i. Injury in Fact

Begin with plaintiff's allegation that he received an increased number of spam calls attempting to extort him. Our court has concluded that increased spam calls after a data breach are not an injury in fact. *Blood*, 2022 WL 11745549, at *6 ("[T]he alleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact."); *see also Legg*, 574 F. Supp. 3d at 993 ("[T]he receipt of phishing emails, while perhaps 'consistent with' data misuse, does not 'plausibly suggest' that any actual misuse of Plaintiff's personal identifying information has occurred." (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)); *In re Practicefirst Data Breach Litig.*, No. 21-CV-00790 (JLS/MJR), 2022 WL 354544, at *5 n.8 (W.D.N.Y. Feb. 2, 2022) (collecting cases and explaining "even if plaintiffs had shown that they received an increase in spam because of this data breach, the Court would still find

these allegations insufficient to allege injury in fact"). Spam calls are annoying. But an annoyance isn't an actual and concrete injury.

An identical fate befalls plaintiff's allegations theorizing that unauthorized actors have tried to access his bank accounts. Plaintiff never pleads that hackers succeeded in their sign-in attempts. *See generally* Doc. 1. He just alleges that he received "multiple notifications" that unknown actors had tried to sign-in into his account. *Id.* at 15 (Compl. ¶ 68). Courts have concluded that receiving notice about attempted logins doesn't constitute an injury in fact. *See De Medicis v. Ally Bank*, No. 21 Civ. 6799 (NSR), 2022 WL 3043669, at *6 (S.D.N.Y. Aug. 2, 2022) ("Plaintiff still fails to establish that he suffered a concrete, particularized injury because the alleged [email account access] attempts were all unsuccessful."); *Kim v. McDonald's USA, LLC*, No. 21-cv-05287, 2022 WL 4482826, at *5 (N.D. Ill. Sept. 27, 2022) (emphasizing that no plaintiff alleged identity theft, and that "notifications that an individual attempted to log in to his email" weren't sufficient (quotation cleaned up)). The unsuccessful sign-in attempts don't qualify as actual and concrete injuries here.

Plaintiff's allegations about financial hacks and purchases fare far better—at least on the injury in fact prong. Recall that plaintiff asserts cybercriminals stole his money by hacking his financial accounts and making unauthorized PayPal purchases. Doc. 1 at 15 (Compl. ¶¶ 68–69). Responding, defendant argues that plaintiff's allegations merely reflect *attempts* at stealing his identity. Doc. 18 at 10. In defendant's view, plaintiff's Complaint suggests he was "reimbursed for any fraudulent transaction, if any actual transaction occurred." *Id.* And, because plaintiff doesn't allege an out-of-pocket loss, defendant suggests, it's not plausible that his identity was stolen. *Id.* But plaintiff needn't allege an out-of-pocket loss to establish an injury in fact. *TransUnion*, 594 U.S. at 425 (recognizing that physical, monetary, and "[v]arious intangible

harms" are sufficiently concrete injuries). Our court already has declined to adopt a theory similar to defendant's argument here, concluding that a data breach plaintiff needn't plead financial harm to show actual injury. *Masterson*, 2023 WL 8647157, at *4 n.4 (rejecting argument "that neither [named plaintiff] has shown an actual injury because neither pleaded that they actually paid the unauthorized charges"). Unauthorized purchases are actual misuses of a plaintiff's PII constituting injuries in fact. *Blood*, 2022 WL 11745549, at *5 (concluding unauthorized bank fees constitute concrete injuries); *In re Progressive*, 2025 WL 213744, at *12–13 (concluding named plaintiffs had alleged actual injury sufficiently from unauthorized charges on debit card); *Masterson*, 2023 WL 8647157, at *4 (assuming that fraudulent debit card charges were concrete and actual injuries). This court reaches the same conclusion here. Plaintiff plausibly has alleged an injury in fact based on his PayPal and financial hacks.

Having established an injury in fact, the court next evaluates whether plaintiff has alleged a causal link between the data breach and plaintiff's injury.

ii. Causation

To establish the requisite causal link, a plaintiff plausibly must allege an injury that's "fairly traceable" to the data breach. *Clapper*, 568 U.S. at 409 (internal quotation marks and citation omitted). And those allegations can't involve a "speculative chain of possibilities[.]" *Id.* at 414; *Masterson*, 2023 WL 8647157, at *3 (same). In other data privacy cases, courts (including this one) have found causation missing when a plaintiff fails to explain how the PII disclosed in the data breach connects to the injury alleged. For example, in *Blood v. Labette County Medical Center*, our court concluded data breach plaintiffs had failed to plead the causation element of standing. 2022 WL 11745549, at *5. There, like here, a data breach allegedly disclosed plaintiffs' names and Social Security numbers. *Id.* at *1. And while

plaintiffs had alleged an injury in fact—unauthorized charges on their bank accounts—they never pleaded "facts suggesting how the mere possession of their Social Security numbers and names would enable someone to make unauthorized charges on an existing account[.]" *Id.* at *5. "To assume someone could have done so with the allegedly stolen information . . . requires a level of speculation and conjecture this Court is unwilling to accept." *Id.*; *see also Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. Aug. 28, 2015) (concluding attempts to open bank accounts and access plaintiff's email not fairly traceable to data breach because stolen data tapes didn't include bank account information and email addresses). Instead, to survive a standing challenge, plaintiff must allege the PII disclosed in *this* data breach was misused, or otherwise show a nonspeculative connection between this data breach and the misuse.

So, how do plaintiff's causation allegations fare here? Plaintiff never pleads allegations that, if true, trace how unauthorized actors could use the disclosed PII (his name, Social Security number, and date of birth) to make unauthorized PayPal purchases or steal his money. But he does explain how cybercriminals develop "complete dossiers on individuals"—known as Fullz packages—by cross-referencing stolen PII with other stolen PII or publicly available data. Doc. 1 at 13–14 (Compl. ¶¶ 61–64). According to plaintiff, creating Fullz packages "means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers." *Id.* at 14 (Compl. ¶ 63). And, plaintiff concludes, "[t]hat is exactly what is happening to Plaintiff[,]" making it "reasonable for any trier of fact . . . to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach." *Id.* (Compl. ¶ 64).

But this causation argument is speculative on two fronts. *First*, plaintiff speculates that unknown cybercriminals took his PII from this data breach and compiled along with other

information to create a Fullz package. *Second*, he implicitly speculates that the Fullz package included plaintiff's financial and PayPal account information, information decidedly not part of *this* data breach. Plaintiff never alleges that his PayPal or bank account information was involved in another data breach or was otherwise publicly available. In fact, he explains that he "stores any documents containing his sensitive PII in safe and secure locations" and "diligently chooses unique usernames and passwords for his various online accounts." *Id.* at 15 (Compl. ¶ 73). Plaintiff's causation theory simply describes Fullz packages as a concept. And then his theory jumps to the conclusion that the information disclosed in the data breach enabled unauthorized actors to access his financial accounts.

Blanket explanations about the development of Fullz packages don't suffice to plead causation. *See Masterson* , 2023 WL 8647157, at *5, *5 n.7 (concluding plaintiffs hadn't established causation where plaintiff never alleged defendant possessed the misused data or "explain[ed] how the combination of PII . . . taken in the data breach . . . combined with 'unregulated data' . . . can lead to the misuse alleged, let alone how that misuse is traceable to [defendant]"); *Zerbe v. IMA Fin. Grp.*, No. 24-2026-HLT-GEB, 2024 WL 3677395, at *6 (D. Kan. Aug. 6, 2024) (concluding in companion case to *Masterson* that the Fullz package allegations weren't sufficient to show "how the combination of some stolen data with unspecified other data available on the internet results in an injury traceable to [defendant]"); *Doe v. Mission Essential Grp.*, No. 23-cv-3365, 2024 WL 3877530, at *7 (S.D. Ohio Aug. 20, 2024) (noting in traceability analysis that "[a]lthough [plaintiff] insists that the PII possibly accessed in the Data Incident" may combine "with other sources to create 'Fullz' packages that can be sold or used to commit fraud[,]" that allegation relies "upon speculation about the actions

of independent actors in combining the PII with information" from other sources). Plaintiff here doesn't "fairly trace" the alleged data breach to Fullz package misuse.[6]

Because plaintiff's alleged instances of past identity theft don't qualify either as injuries in fact or as fairly traceable to the data breach, plaintiff hasn't shown the all-important "actual misuse" required to plead standing. *See Blood*, 2022 WL 11745549, at *8 (concluding the court had "no sufficient allegations of data misuse" when each allegation of misuse failed as either an injury in fact or as fairly traceable to the data breach). Next, the court considers whether plaintiff's future identity theft allegations can qualify as an injury in fact.

b. Risk of Future Identity Theft and Fraud

Plaintiff takes his identity theft and fraud allegations one step further, alleging he faces "imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from [his] PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals." Doc. 1 at 16 (Compl. ¶ 75). Defendant argues that these allegations merely speculate about future events and conduct of unknown third parties, which undercut plaintiff's risk of future harm. Doc. 18 at 11.

Before the court applies case law to evaluate plaintiff's allegations of future risk, the court clarifies an important, orienting principle: Risk of future identity theft *alone* doesn't confer standing for *damages* claims. *TransUnion*, 594 U.S. at 437 (finding mere risk of future harm—without showing the risk had materialized—doesn't suffice to confer standing for damages claims). So, one might ask, why should the court evaluate that risk here? A cognizable risk of

[6] Plaintiff identifies three out-of-circuit cases accepting allegations about Fullz packages as plausible explanations of traceability. *See* Doc. 20 at 10 (first citing *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 792 (W.D. Wis. 2019); then citing *Flores v. Aon Corp.*, 242 N.E. 3d 340, 354 (Ill. App. Ct. 2023); and then citing *In re GEICO Customer Data Breach Litig.*, No. 21-CV-2210-KAM-SJB, 2023 WL 4778646, at *6–7 (E.D.N.Y. July 21, 2023)). The court doesn't find these cases persuasive on the facts alleged here, given our court's rejection of a similar theory in other cases.

future harm may suffice for plaintiff to allege a past injury in fact based on his emotional distress and mitigation efforts. *See below* § III.B.2–3. The court evaluates plaintiff's standing based on those alleged injuries later in this Order. But, first, the court examines the threshold question: whether plaintiff has alleged sufficiently a risk of future identity theft.

Other Circuits have developed a three-factor test to determine "when the risk of future misuse of PII following a data breach is imminent and substantial." *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375 (1st Cir. 2023). Those three factors are:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain the 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.

McMorris, 995 F.3d at 303.[7] These factors aren't exclusive. *Id.* And, in the First Circuit's view, they aren't "necessarily determinative[.]" *Webb*, 72 F.4th at 375. "[B]ut they do provide guidance." *Id.*

Our court also has evaluated these three factors—even after concluding a plaintiff's failure to allege misuse "alone puts plaintiff on shaky standing grounds." *F.S. v. Captify Health, Inc.*, No. 23-1142-DDC-BGS, 2024 WL 1282437, at *4 (D. Kan. Mar. 26, 2024). The court takes the same approach again, here. It concludes plaintiff hasn't shown an imminent risk of future identity theft.

i. Targeted Attempt

First, consider whether the breach resulted from an intentional, targeted effort. To be sure, "all cyber-attacks involve some degree of intentional conduct just by the very nature of the

[7] The First, Second, and Third Circuits all consider these three factors. *See Webb*, 72 F.4th at 375–77; *Bohnak*, 79 F.4th at 283 (reaffirming three *McMorris* factors post-*TransUnion*); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153–54, 157 (3d Cir. 2022).

attack." *In re Samsung Data Sec. Breach Litig.*, No. 23-md-03055, 2025 WL 271059, at *6 (D.N.J. Jan. 3, 2025) (internal quotation marks and citation omitted). But a clearly "intentional breach makes standing more likely." *Alonzo v. Refresco Beverages US, Inc.*, No. 23-22695 (GC) (JBD), 2024 WL 4349592, at *5 (D.N.J. Sept. 30, 2024) (citing *McMorris*, 995 F.3d at 301).

Here, plaintiff attaches the data breach letter distributed by defendants to his Complaint.[8] *See* Doc. 1-1 at 2 (Pl. Ex. 1). The letter repeatedly used the passive voice to explain the data breach incident: "[T]here was unauthorized access to [defendant's] network" and "certain files and folders were viewed or taken without authorization[.]" *Id.* Plaintiff interprets this language to mean that "cybercriminals obtained everything they needed to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals[.]" Doc. 1 at 2 (Compl. ¶ 8). But that interpretation seems like a leap, given the information provided in defendant's letter. And there's no indication plaintiff has any other information to support his conclusory allegation. *Cf. Deevers v. Wing Fin. Servs., LLC*, No. 22-CV-550-CVE-JFJ, 2023 WL 6133181, at *5 (N.D. Okla. Sept. 19, 2023) (explaining that it's "unclear" whether plaintiffs sufficiently alleged a targeted attack because they just had alleged unauthorized parties could access client records and defendant identified unauthorized access, but plaintiffs didn't "allege that a specific third party actor stole information, or that a known third party targeted" the systems). The court thus acknowledges the possibility of a targeted attack by cybercriminals, as plaintiff alleges, but doesn't unqualifiedly accept it as true. *See Blood*, 2022 WL 11745549, at *3 (explaining that "a court need not accept conclusory allegations" as true at the pleading stage (quotation cleaned

[8] "Exhibits attached to a complaint are properly treated as part of the pleadings for purposes of ruling on a motion to dismiss." *Tal v. Hogan*, 453 F.3d 1244, 1264 n.24 (10th Cir. 2006) (evaluating plaintiff's exhibits in ruling a 12(b)(6) motion). A facial 12(b)(1) challenge proceeds under the "same standards" as a 12(b)(6) motion to dismiss. *Muscogee (Creek) Nation v. Okla. Tax Comm'n*, 611 F.3d 1222, 1227 n.1 (10th Cir. 2010).

up)). And so, the first factor slightly favors finding an injury in fact from plaintiff's future identity theft allegations.

ii. Misuse

Second, the test directs courts to consider whether plaintiff has alleged any portion of the dataset was misused. As established above, plaintiff's alleged misuses fall short of the mark because they don't qualify either as injuries in fact or as fairly traceable to the data breach. So, this factor significantly cuts against finding a "certainly impending" future injury. *Clapper*, 568 U.S. at 409 (quotation cleaned up).

While some cases conclude misuse isn't an essential part of the test, sister district courts in the Tenth Circuit emphasize the vitality of misuse to the standing calculus. In fact, some don't evaluate the other two factors at all and concentrate solely on actual misuse at the future harms stage, as well. *Compare Bohnak*, 79 F.4th at 289 ("[A known misuse of information] allegation is not necessary to establish that an injury is sufficiently imminent to constitute an injury in fact."); *with Masterson*, 2023 WL 8647157, at *8 (emphasizing the importance of actual misuse in risk of future injuries analysis to show a data breach injury is concrete, particularized, or imminent without evaluating other two factors); *and Deevers*, 2023 WL 6133181, at *5–6 (applying three factors and explaining "the majority of courts, including district courts in this circuit, have concluded that plaintiffs must allege actual misuse . . . to demonstrate they face an imminent risk of fraud"). Indeed, our court has *required* some form of actual misuse to show an imminent and substantial risk of future harm in data privacy cases. *See Blood*, 2022 WL 11745549, at *7–8 (evaluating plaintiff's allegations of actual misuse and whether those allegations support an injury in fact based on risk of future identity theft); *see also In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021), *cert. denied sub*

nom. Huang v. Spector, 142 S. Ct. 431 (2021) (finding plaintiffs plausibly had alleged an injury in fact because some plaintiffs already had their identities stolen already and the "the allegations of some Plaintiffs that they have suffered injuries resulting from *actual* identity theft support the sufficiency of all Plaintiffs' allegations that they face a *risk* of identity theft" (emphasis in original)). This factor—a weighty one for district courts in our Circuit—significantly undercuts plaintiff's future-risk-of-identity-theft argument.

iii. Sensitive Data

Third, consider whether data exposed in the breach is susceptible to fraud. Plaintiff alleges his name, Social Security number, and date of birth were exposed in the breach. Doc. 1 at 14 (Compl. ¶ 66). This data is precisely the type of sensitive, high-risk information susceptible to fraud. *McMorris*, 995 F.3d at 302 ("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."). This factor favors a conclusion that plaintiff has alleged a sufficient injury in fact.

As the First Circuit explained, the three factors "are neither exclusive nor necessarily determinative, but they do provide guidance." *Webb*, 72 F.4th at 375. Next, the court evaluates one last factor before deciding whether plaintiff has alleged a "certainly impending" risk of future identity theft. *See Clapper*, 568 U.S. at 409 (quotation cleaned up).

iv. Miscellaneous Consideration

Aside from allegations of identity theft, plaintiff attempts to show imminence by citing a plethora of research and reports about identity theft crimes and data breaches. *See* Doc. 1 at 12–14, 17 (Compl. ¶¶ 57–63, 81). But this court already has rejected this approach, concluding it doesn't establish a cognizable risk of future harm. *See Med-Data Inc.*, 2022 WL 970862, at *7

(finding that plaintiffs hadn't pleaded "any particularized facts to corroborate" fear of future identity theft and "research and reports about identity theft crimes" don't suffice to show a risk of future harm); *Legg*, 574 F. Supp. 3d at 993 (finding that plaintiff "relies on reports that describe the general risks of identity theft, explain how personal information can be sold on illicit internet cites, and identify other data breaches" but those reports "'do nothing to clarify the risks to the plaintiffs in this case'" (quoting *Tsao*, 986 F.3d at 1343)). Simply put, the referenced reports don't persuade the court that the threatened injury is "certainly impending." *Clapper*, 568 U.S. at 409 (quotation cleaned up).

At bottom, the court concludes plaintiff hasn't alleged a risk that future identity theft is imminent. While the data's sensitivity favors an injury in fact conclusion, the court isn't convinced plaintiff's allegations about cybercriminals and a targeted attack move beyond the conclusory stage. And the alleged misuse factor—arguably the most important factor—strongly disfavors concluding that plaintiff has alleged a sufficient injury in fact. Finally, plaintiff's attempt to lean into research and reports doesn't help his cause. Without the alleged misuse, his threats of future identity theft are too speculative to confer standing.

But even if one assumes plaintiff had alleged sufficiently a risk of future identity theft, that risk wouldn't confer standing for *damages* automatically. That's because, recall, future identity theft *alone* doesn't suffice as an injury in fact for damages. *TransUnion*, 594 U.S. at 436–37. But sometimes, a risk of future harm can couple with other harms to create a cognizable injury in fact supporting damages. Plaintiff seeks damages from two harms that fit this bill: emotional distress and mitigation efforts. So, the court evaluated plaintiff's future injury allegations as a potential companion to establish standing under emotional distress and

mitigation efforts. The court's conclusion—that plaintiff hadn't alleged a future risk of identity theft—thus dooms plaintiff's emotional distress and mitigation injuries.

2. Emotional Distress

Plaintiff alleges he experienced fear and anxiety from the loss of his privacy. Doc. 1 at 16 (Compl. ¶ 74). And, he alleges, he will continue suffering emotional distress. *Id.* (Compl. ¶ 79). Defendant responds, contending that this emotional distress won't support standing unless plaintiff also has alleged an impending risk of future identity theft or actual misuse of the PII disclosed in the data breach. Doc. 18 at 13. Defendant is correct—emotional distress *plus* actual misuse or certainly impending future harm can qualify as an injury in fact. *Masterson*, 2023 WL 8647157, at *7 ("[T]here are no allegations of misuse tied to [defendant]. And, . . . there is no risk of future harm that is certainly impending or substantial. Based on this, Plaintiffs' bare-bones allegations of emotional distress are not sufficient to confer standing."). Plaintiffs can't "manufacture standing merely by inflicting harm on themselves[.]" *Clapper*, 568 U.S. at 416. Absent allegations of actual misuse or an imminent threat of future harm, emotional distress allegation can't qualify as a present or future harm sufficient for standing.

His next asserted injury suffers the same fate.

3. Lost Time from Mitigation Efforts

Plaintiff alleges he spent 240 hours mitigating the data breach's consequences. Doc. 1 at 15 (Compl. ¶ 71). In those hours, he verified the legitimacy of the Notice of Data Breach, self-monitored his accounts, reviewed his credit reports, and otherwise "mitigat[ed] fraud and identity theft." *Id.* But mitigation time constitutes a concrete injury only if it's "based on a threat of future injury that is certainly impending." *Blood*, 2022 WL 11745549, at *6 (concluding mitigation time not an injury in fact after concluding plaintiffs hadn't alleged fraud injuries fairly

traceable to the data breach); *Legg*, 574 F. Supp. 3d at 994 ("[W]hile it may have been reasonable to take some steps to mitigate the risks associated with the data breach, those actions cannot create a concrete injury where there is no imminent threat of harm."); *Stern*, 2025 WL 239036, at *7 ("Plaintiffs' fear about misuse of their PII is not certainly impending harm, as no Plaintiff has alleged that their data is actually available on the dark web or otherwise has been transmitted to others for imminent use."). Without actual misuse or a certainly impending threat of future injury, plaintiff again "manufacture[s] standing merely by inflicting harm on [himself] based on [his] fears of hypothetical future harm[.]" *Clapper*, 568 U.S. at 416. That's not sufficient to constitute an injury in fact—for past mitigation efforts or future ones.

Last up, the final injury allegation to support damages—lost privacy.

4. Lost Privacy

Plaintiff alleges defendant "affirmatively and recklessly disclosed" plaintiff's PII to "unauthorized third parties." Doc. 1 at 31 (Compl. ¶ 147). And defendant's "reckless and negligent failure to protect Plaintiff and Class Members' PII constitutes an intentional interference with [their] interest in solitude or seclusion . . . [in a manner] that would be highly offensive to a reasonable person." *Id.* at 31–32 (Compl. ¶ 149). Based on these allegations, the court interprets plaintiff's lost privacy claim here as one sounding in the intrusion upon seclusion tort. So, the court next evaluates whether these intrusion upon seclusion allegations confer standing.

Remember, standing requires an injury that is both actual or imminent, *and* concrete. *Lujan*, 504 U.S. at 560. The court has referenced many cases that—when evaluating commonly alleged data breach injuries—fail to distinguish between those two injury-in-fact requirements. But when evaluating a lost privacy harm, the distinction comes into focus. While a plaintiff may

allege an *actual* loss of privacy resulting from a data breach, that doesn't mean their asserted injury is *concrete*. So, the court's analysis now must focus on the concreteness of plaintiff's alleged lost privacy.[9]

The Supreme Court has clarified that concrete injuries are those with "a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *TransUnion*, 594 U.S. at 424 (quotation cleaned up). And to identify such a traditionally recognized harm, the Supreme Court has looked to the Restatement of Torts. *Id.* at 432 (referencing the Restatement when assessing whether the alleged injury bore a "close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts" on the concrete harm requirement (internal quotation marks and citation omitted)). The Restatement outlines four, traditionally distinct privacy torts: (1) intrusion upon seclusion; (2) appropriation of name or likeness; (3) public disclosure of private facts; and (4) false light publicity. *See* Restatement (Second) of Torts § 652A (Am. L. Inst. 1977) (October 2024 Update). As *TransUnion* explained, "disclosure of private information, and intrusion upon seclusion" may constitute concrete, intangible harms. 594 U.S. at 425.[10] The court evaluates

---

[9] As a case in point, plaintiff here focused his briefing on whether his loss of privacy injury was actual or imminent. *See* Doc. 20 at 5 ("'To sustain an injury based on loss of privacy, other courts have required some allegation that personal information has been viewed of exposed in a way that would facilitate easy, imminent access.'" (quoting *Masterson*, 2023 WL 8647157, at *7)); *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28–29 (D.D.C. 2014) (concluding invasion of privacy didn't satisfy *imminence* requirement when plaintiff hadn't alleged their PII was viewed or "exposed in a way that would facilitate easy, imminent access").

Taking plaintiff's allegations as true, the court assumes an actual or imminent loss of privacy injury under the definitions used in these cases. Nonetheless, his loss of privacy allegations still don't establish injury in fact because they aren't concrete, as the court explains in this section.

[10] In the data breach context, courts—including ours—have evaluated loss of privacy for standing purposes by comparison to the public disclosure of private facts tort. *See Med-Data, Inc.*, 2022 WL 970862, at *9 ("Plaintiff's alleged loss of privacy damages here arise from her invasion of privacy tort claim—specifically, the tort of public disclosure of private information." (quotation cleaned up)); *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *8 ("[E]ven if plaintiffs could plead facts sufficient

whether plaintiff's alleged lost privacy injury here establishes standing because of its close relationship to the intrusion upon seclusion tort.

The Restatement provides:

> One who *intentionally* intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (Am. L. Inst. 1977) (October 2024 Update) (emphasis added). "[O]ne who suffers an intrusion upon his solitude or seclusion, under § 652B, may recover damages for the deprivation of his seclusion." *Id.* § 652H cmt. a. "While plaintiffs are not required to prove the elements for a common-law analogue in order to secure standing, they must demonstrate that the harm posed by the theft of their information bears a close relationship to these traditionally recognized harms." *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (quotation cleaned up).

Here, plaintiff's intrusion upon seclusion claim falls short of the requisite close relationship because intent is absent. According to plaintiff, defendant "acted with a knowing

---

to allege the tort of public disclosure of private information, the Court would still find a lack of subject matter jurisdiction here. Indeed, this theory of standing has been rejected in the data breach context where, like in this case, plaintiffs have failed to demonstrate any concrete or particularized injury associated with the disclosure.").

Our court also has emphasized that, in a claim for public disclosure of private facts, "loss of privacy, in and of itself, is not a concrete harm that can provide the basis for Article III standing." *Med-Data Inc.*, 2022 WL 970862, at *10. So, even if the court construed plaintiff's claim as one for public disclosure of private facts, plaintiff hasn't alleged actual harm fairly traceable to the data breach. So, loss of privacy wouldn't confer standing.

Nonetheless, the court construes plaintiff's claim as one of intrusion upon seclusion. Doc. 1 at 31–32 (Compl. ¶ 149) (alleging defendant's conduct intentionally interfered with plaintiff's "interest in solitude or seclusion"); Doc. 20 at 14 (responding to motion to dismiss invasion of privacy claim by recounting the elements of an intrusion upon seclusion claim). And so, this section engages in an intrusion upon seclusion analysis.

state of mind when it permitted the Data Breach because it knew its information security practices were inadequate." *Id.* at 32 (Compl. ¶ 150). But as defendant emphasizes, plaintiff can't "tie any alleged privacy invasion to [defendant] rather than the criminal cyberattackers." Doc. 18 at 12. Plaintiff doesn't allege defendant *intentionally* permitted a third party to intrude his seclusion. He simply alleges defendant knew its security systems were inadequate, and therefore "permitted the Data Breach[.]" Doc. 1 at 32 (Compl. ¶ 150). But the intrusion upon seclusion tort traditionally permitted recovery only when the defendant intentionally had invaded the plaintiff's private affairs. Even viewing plaintiff's nonconclusory allegations in the light most favorable to him, he hasn't alleged an intentional invasion by defendant.

The court thus concludes plaintiff's harm resulting from the data breach doesn't bear a close relationship to the type of harm contemplated under the intrusion upon seclusion tort. *See Zynga*, 600 F. Supp. 3d at 1050 n.10 (deciding standing on other grounds but noting that "it is doubtful whether [plaintiffs] can show that Zynga (whom plaintiffs sue for negligence) directly harmed them in a way that is analogous to the harm from *intentional* intrusion upon seclusion" because plaintiffs alleged a third-party stole their PII (emphasis in original)). Plaintiff's loss of privacy injury—even if actual and imminent—isn't concrete and thus doesn't suffice as an injury in fact.

For his damages claims, plaintiff hasn't alleged any injuries in fact fairly traceable to the data breach. That means he doesn't have standing to seek damages. But recall that "plaintiffs must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *TransUnion*, 594 U.S. at 431. Having

addressed plaintiff's standing to seek damages, the court next must evaluate plaintiff's standing to seek injunctive and declaratory relief.[11]

C. Injunctive & Declaratory Relief

Remember, a "threatened injury must be certainly impending to constitute an injury in fact." *Clapper*, 568 U.S. at 409 (quotation cleaned up). "Allegations of possible future injury are not sufficient." *Id.* (quotation cleaned up); *TransUnion*, 594 U.S. at 435 ("[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."). The "threat of injury must be both real and immediate, not conjectural or hypothetical." *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983) (quotation cleaned up).

In the current case, plaintiff asks the court to declare: (1) defendant owes a duty to secure the proposed class's PII; (2) defendant continues to breach that duty by failing to employ reasonable measures to secure the proposed class's PII; and (3) these ongoing breaches continue to cause the proposed class harm. Doc. 1 at 39 (Compl. ¶ 191). And he asks for "corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols . . . to protect consumers' PII." *Id.* (Compl. ¶ 192). Has plaintiff alleged an injury in fact sufficient to seek this injunctive and declaratory relief?

First, an important point about the future injury undergirding this injunctive and declaratory relief: the injury supporting this relief is not *future* misuse of the PII already disclosed in the breach. Instead, it's the risk that defendant will face *another* data breach, and

[11] The parties didn't focus much of their efforts on this topic. *See* Doc. 18 at 15 (briefly explaining that prospective injunctive relief wouldn't redress plaintiff's alleged future risk of identity theft); Doc. 20 at 11–12 (briefly suggesting an ongoing risk of another data breach); *id.* at 15 (explaining why declaratory relief is available). The court aligns itself with the parties' approach and addresses these forms of relief more briefly.

release plaintiff's PII into the world again. *See In re Progressive*, 2025 WL 213744, at *13 ("Here, the complained of harm supporting an injunction is that [defendant] will experience another data breach and further compromise Plaintiffs' PII."); *see also Webb*, 72 F.4th at 378 ("[A]n injunction requiring [defendant] to improve its cybersecurity systems cannot protect the plaintiffs from future misuse of their PII by the individuals they allege now possess it."). An injunction couldn't remedy future misuse of data already in the hands of unknown third parties.

In a strikingly similar situation, the District of Utah recently concluded plaintiffs lacked standing to seek injunctive relief. *In re Progressive* concluded that plaintiffs "failed to plausibly allege that there is a substantial risk of another breach of [defendant's] systems or that a breach is certainly impending." 2025 WL 213744, at *14. To be certain, the plaintiffs had alleged that defendant stored plaintiffs' data in an unencrypted, internet-accessible system. *Id.* And, they also emphasized, in the wake of the data breach, defendant didn't remove the PII from that system or add encryption. *Id.* What's more, the plaintiffs alleged, defendant's security was still inadequate. *Id.* But defendant "publicly denie[d] these allegations." *Id.* In the court's view, though, the complaint's allegations didn't show defendant faced a greater risk of a data breach than "any other entity that holds PII." *Id.* The court explained that—if the court concluded these allegations sufficed to establish an imminent risk of future injury—"'virtually every company and government agency might be exposed to requests for injunctive relief like the one the plaintiffs seek here.'" *Id.* (quoting *Webb*, 72 F.4th at 378); *see also Hall v. Centerspace, LP*, No. 22-cv-2028 (KMM/DJF), 2023 WL 3435100, at *3–4 (D. Minn. May 12, 2023) (concluding plaintiff fell short of proving a future data breach was imminent—he hadn't alleged hackers were presently targeting defendant or otherwise shown defendant was "uniquely vulnerable to incursions"—so he didn't have standing to seek injunctive and declaratory relief); *cf. In re*

MOVEit Customer Data Sec. Breach Litig., No. 23-md-03083-ADB-PGL, 2024 WL 5092276, at *3 n.3 (D. Mass. Dec. 12, 2024) (briefly addressing redressability and emphasizing that the "Court agrees that many of Plaintiffs' claims for injunctive relief require dismissal because prospective remedies targeting the named Defendants cannot address the risk of future harm caused by the Data Breach").

This case is a close cousin to *In re Progressive*. Plaintiff here likewise alleges that defendant "elected to store the unencrypted PII . . . in an Internet-accessible environment[.]" Doc. 1 at 7 (Compl. ¶ 37). And, according to plaintiff, defendant's "data security measures remain inadequate[,]" but defendant "publicly denies these allegations." *Id.* at 38 (Compl. ¶ 189). Simply put, plaintiff alleges it doesn't know of any efforts defendant has made to protect his sensitive PII in the aftermath of the breach. *Id.* But the data breach notice—attached to plaintiff's Complaint—indicates the company "confirm[ed] the security" of its systems, "reported this event to federal law enforcement[,]" and was "reviewing [its] policies, procedures, and processes to reduce the likelihood of a similar future event." Doc. 1-1 at 2 (Pl. Ex. 1). These efforts "cut against any inference that defendant's prior data breach might make a future data breach more likely." *Scifo v. Alvaria, Inc.*, No. 23-cv-10999-ADB, 2024 WL 4252694, at *5 n.10 (D. Mass. Sept. 20, 2024) (quotation cleaned up) (finding plaintiff's standing to seek injunctive relief undercut by notice indicating defendant secured its networks, initiated enhanced security measures, sought forensic investigation assistance, and notified the FBI). The court finds that plaintiff here hasn't alleged any more to show a future data breach is "certainly impending" than plaintiffs in *In re Progressive*. *Clapper*, 568 U.S. at 409 (quotation cleaned up).

And so, the court concludes plaintiff lacks standing to seek his requested injunctive and declaratory relief.

IV. Conclusion

Taking stock of all plaintiff's alleged injuries and requested relief, plaintiff doesn't have standing to maintain this suit. Plaintiff must support his damages request with an injury in fact. But at every alleged injury specific to plaintiff, the Complaint's allegations fall short. Plaintiff hasn't alleged actual misuse of his stolen PII that is fairly traceable to the data breach. He hasn't shown that the risk of future identity theft and fraud is sufficiently imminent. And his emotional distress, mitigation costs, and loss of privacy aren't cognizable injuries in fact. Plaintiff also lacks standing to seek injunctive and declaratory relief against defendant because he hasn't shown another data breach is imminent.

Without standing, there's no Article III case or controversy before the court. In turn, that conclusion means that the court lacks subject matter jurisdiction over this action.

IT IS THEREFORE ORDERED THAT defendant's Motion to Dismiss (Doc. 17) is granted. Plaintiff's Complaint is dismissed without prejudice.

IT IS SO ORDERED.

Dated this 5th day of March, 2025, at Kansas City, Kansas.

s/ Daniel D. Crabtree
Daniel D. Crabtree
United States District Judge