UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA

Robert Devine v. Horizontal Integration, Inc.

No. 24-CV-4555 (D. Minn. Dec. 19, 2025) · No. 0:24-cv-04555 · Decided December 19, 2025

SUMMARY

The United States District Court for the District of Minnesota granted without prejudice a defendant's motion to dismiss claims arising from a data breach. The court held that the plaintiff failed to adequately allege Article III standing because he did not identify what personal information was disclosed, establish a substantial risk of future harm, or show that alleged spam, credit-related harm, emotional distress, and other injuries were fairly traceable to the breach. The court dismissed the action for lack of subject-matter jurisdiction and did not reach the Rule 12(b)(6) arguments.

CASE DETAILS

COURT	United States District Court for the District of Minnesota
WRITING FOR THE COURT	Jeffrey M. Bryan
JURISDICTION	United States District Court for the District of Minnesota
DECIDED	December 19, 2025
DOCKET	0:24-cv-04555
DISPOSITION	dismissed
PROCEDURAL POSTURE	Motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) and failure to state a claim under Rule 12(b)(6).
STANDARD OF REVIEW	De novo for a motion to dismiss for lack of subject matter jurisdiction.
PRECEDENTIAL VALUE	unpublished

TOPICS

standing · subject matter jurisdiction · motions to dismiss · civil procedure · due process

PRACTICE AREAS

civil procedure · constitutional law · consumer protection

QUESTIONS PRESENTED

1. Whether plaintiff has Article III standing to pursue claims arising from a data breach where the complaint does not allege that plaintiff's own personal identifiable information or protected health

information was disclosed in the breach.

2. Whether allegations of future risk of identity theft, increased spam, credit score decline, time spent monitoring accounts, diminished value of PII/PHI, and emotional distress are sufficient to establish concrete injury in fact and traceability for standing purposes.

HOLDINGS

1. Plaintiff lacks standing for equitable relief because the complaint fails to establish a 'certainly impending' or 'substantial risk' of a future data breach absent the injunctive relief sought.
2. Plaintiff lacks standing for monetary damages because the complaint fails to identify what of plaintiff's own information was accessed or taken in the data breach, and thus fails to allege concrete or particularized harm from loss of privacy.
3. The complaint fails to plausibly plead traceability between increased spam emails and the data breach because it contains no allegations that plaintiff's email address was disclosed, does not describe the subject matter of the emails, and alleges only that spam occurred 'in the aftermath' of the breach.
4. Plaintiff's allegations of credit score decline and unauthorized inquiries are not fairly traceable to the data breach because credit scores can lower for a variety of reasons, and the timing allegations ('shortly after' and 'following') are insufficient to establish causation.
5. Time spent monitoring accounts does not create standing when the plaintiff has not established a substantial and imminent risk of identity theft, because a plaintiff cannot manufacture standing by inflicting harm on themselves based on fears of hypothetical future harm.
6. Allegations of diminished value of PII/PHI and lost benefit of the bargain are too general and conclusory to plausibly plead an injury in fact where the complaint does not identify the specific PII/PHI disclosed or explain how its monetary value was reduced.
7. Emotional distress allegations are not fairly traceable to the data breach absent allegations that plaintiff's own PII/PHI was disclosed and that this disclosure caused the emotional distress.

KEY QUOTATIONS

> *"The universal interest in the security of one's private data does not equate to a substantial and imminent risk of harm."*

> *"If that risk were deemed sufficiently imminent to justify injunctive relief, virtually every company and government agency might be exposed to requests for injunctive relief like the one the plaintiffs seek here."*

> *"A plaintiff 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'"*

> *"Simply alleg[ing] that [an] [injury] happened after the . . . breach does not 'sufficiently connect' the Data Breach to the injury."*

FACTUAL BACKGROUND

Plaintiff Robert Devine, a former employee of defendant Horizontal Integration, Inc. (a digital marketing and staffing services business), brought a putative class action after a data breach where third-party hackers accessed Horizontal's systems between July 3-11, 2024. The breach potentially affected over 6,345 individuals' personal information, including names, Social Security numbers, and financial information. Devine received a notice in October 2024 but alleged the notice did not specify what of his personal information was compromised. Devine alleged experiencing a spike in spam emails, receiving a suspicious email about his credit report, and discovering his credit score had dropped.

PROCEDURAL HISTORY

Plaintiff filed a putative class action complaint and amended complaint asserting claims for negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, and violation of the Minnesota Uniform Deceptive Trade Practices Act. Defendant moved to dismiss under Rules 12(b)(1) and 12(b)(6).

DISPOSITION

dismissed

REMAND INSTRUCTIONS

Dismissed without prejudice for lack of standing. Judgment to be entered accordingly.

CASES CITED

- City of Clarkson Valley v. Mineta, 495 F.3d 567 (8th Cir. 2007)
- Alleruzzo v. SuperValu, Inc. (In re SuperValu, Inc. Customer Data Sec. Breach Litig.), 870 F.3d 763 (8th Cir. 2017)
- Spokeo v. Robins, 578 U.S. 330 (2016)
- TransUnion LLC v. Ramirez, 594 U.S. 413 (2021)
- Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)
- Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), 528 U.S. 167 (2000)
- Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)
- Thomas v. Pawn Am. Minn., LLC (In re Pawn), No. 21-CV-2554 (PJS/JFD), 2022 WL 3159874 (D. Minn. Aug. 8, 2022)
- Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365 (1st Cir. 2023)
- Perry v. Bay & Bay Transp. Servs., Inc., 650 F. Supp. 3d 743 (D. Minn. 2023)
- Berry v. Crescent Cmty. Health Ctr., No. 24-CV-1036 (CJW/KEM), 2025 WL 1287909 (N.D. Iowa May 2, 2025)
- Blood v. Labette Cnty. Med. Ctr., No. 5:22-CV-4036 (HLT/KGG), 2022 WL 11745549 (D. Kan. Oct. 20, 2022)
- Legg v. Leaders Life Ins. Co., 574 F. Supp. 985 (W.D. Okla. 2021)

- In re Practicefirst Data Breach Litig., No. 1:21-CV-00790 (JLS/MJR), 2022 WL 354544 (W.D.N.Y. Feb. 2, 2022)
- Welborn v. Internal Revenue Servs., 218 F. Supp. 3d 64 (D.C.C. 2016)
- McCombs v. Delta Grp. Elec., Inc., 676 F. Supp. 3d 1064 (D.N.M. 2023)
- Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564 (D. Md. 2016)
- Priddy v. Zoll. Med. Corp., No. 1:23-CV-10575-IT, 2025 LEXIS 62112 (D. Mass. Mar. 31, 2025)
- In re Marriott Int'l, Inc., 440 F. Supp. 3d 447 (D. Md. 2020)
- Plaintiffs v. MGM Resorts Int'l, 638 F. Supp. 3d 1175 (D. Nev. 2022)
- In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2904, 2021 WL 5937742 (D.N.J. Dec. 16, 2021)

OPINION

Devine

PER CURIAM.

UNITED STATES DISTRICT COURT

DISTRICT OF MINNESOTA

Robert Devine, on behalf of himself and all File No. 24-CV-4555 (JMB/DLM) others similarly situated, Plaintiff, v. ORDER Horizontal Integration, Inc., doing business as Horizontal Digital and Horizontal Talent, Defendants. Brittany N. Resch, Carolyn Chen (pro hac vice), and Raina Borrelli, Strauss Borrelli PLLC, Chicago, IL, for Plaintiff Robert Devine. Daniel P. Brees and Ellen A. Brinkman, Gordon Rees Scully Mansukhani, LLP, Minneapolis, MN; and John T. Mills (pro hac vice), Joseph Salvo (pro hac vice), and R. Michael Riecken (pro hac vice), Gordon Rees Scully Mansukhani, LLP, New York, NY; for Defendant Horizontal Integration, Inc. This matter is before the Court on Defendant Horizontal Integration, Inc.'s Motion to Dismiss Plaintiff Robert Devine's claims against it for lack of standing under Federal Rule of Civil Procedure 12(b)(1) and for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6). (Doc. No. 14.) For the reasons explained below, the Court grants the motion to dismiss without prejudice for lack of standing.

BACKGROUND

A. The Parties Horizontal is a digital marketing and professional staffing services business headquartered in St. Louis Park, Minnesota. (Doc. No. 13 [hereinafter "Am. Compl."] ¶¶ 2, 9, 13.) Devine is a former Horizontal employee and Minnesota resident. (Id. ¶¶ 8, 35.) The Amended Complaint includes allegations that Horizontal collected "significant amounts of" personal identifiable information (PII) and protected health information (PHI) from Devine, including, but not limited to, his name, Social Security number, phone number, and email address. (Id. ¶ 35.)1 B. The Data Breach On or about July 9, 2024, Horizontal detected unusual activity in its network and worked with third-party cybersecurity specialists to secure its system. (Id. ¶ 18; see also id. ¶ 18 n.10 (including a link to a document titled "Notice of Data Event" from the New Hampshire

Attorney General [hereinafter, "Notice"] at 1).) Horizontal's investigation into the activity revealed that, between July 3, 2024, and July 11, 2024, third-party hackers "accessed or t[ook]" certain files from its system [hereinafter, "Data Breach"]). (Notice at 1.) Horizontal's review of the data at risk revealed that "certain personal information" of its current and former employees may have been affected. (Id.; Am. Compl. ¶¶ 3, 14.) More specifically, they learned that the following types of personal information "could [have] be[en] affected": names, phone numbers, email addresses, Social Security numbers, driver's license numbers, financial account information, credit card numbers, debit card numbers, and health information. (Notice at 1; Am. Compl. ¶¶ 20, 21; see also id. ¶ 20 n.13 [hereinafter "Texas Breach Report"].) It also learned that at least 6,345 individuals 1 The Amended Complaint does not specify what PHI Horizontal is alleged to have collected. were potentially affected. (Id. ¶ 23; see also id. ¶ 23 n.14 [hereinafter "Maine Data Breach Notification"]; Notice at 2.) On or about July 24, 2024, Horizontal began notifying the potentially affected individuals it had identified. (Notice at 4–11.) On October 29, 2024, after identifying more potentially affected individuals, it sent a supplemental notice to those individuals. (Id. at 1–2, 13–16.) Devine received the October notice. (Am. Compl. ¶¶ 6, 29, 40; Notice at 1– 2, 13–16.) The notice did not specify the type of personal information affected. (Am. Compl. ¶ 29; Notice at 1–2, 13–16.) The notice specified, however, that Horizontal was offering those "who may have had personal information potentially impacted" free "access to credit monitoring services . . . through Experian." (Notice at 2.) Devine alleges that after the Data Breach he suffered from "a spike in spam and scam emails" (Am. Compl. ¶ 45), received an email from someone who "purported to be Experian" who "claimed that his credit report had been subject to an excessive amount of [unauthorized] inquiries" (id. ¶ 52), and "discovered his credit score had dropped to . . . a number . . . lower than what it had been" before the Data Breach. (Id. ¶ 53.) C. This Action Devine commenced this action in December 2024 (Doc. No. 1), and the Amended Complaint asserts the following six claims on behalf of himself and others: negligence (Count I) (Am. Compl. ¶¶ 94–114), negligence per se (Count II) (id. ¶¶ 115–26), breach of implied contract (Count III) (id. ¶¶ 127–43), invasion of privacy (Count IV) (id. ¶¶ 144– 57), unjust enrichment (Count V) (id. ¶¶ 158–67), and violation of the Minnesota Uniform Deceptive Trade Practices Act (MDTPA) (Count VI) (id. ¶¶ 168–78).

DISCUSSION

Defendant has moved to dismiss Plaintiff's claims for lack of standing and for failure to state a claim. Because the Amended Complaint contains inadequate factual allegations concerning the alleged injury, the Court grants the motion for lack of standing. Horizontal argues that Devine lacks standing to pursue any of his claims under Article III of the U.S. Constitution. (Doc. No. 16 at 5–17.) Standing is a jurisdictional prerequisite; as a result, it must be established before this Court can reach the merits of Devine's claims. City of Clarkson Valley v. Mineta, 495 F.3d 567, 569 (8th Cir. 2007); see also Fed. R. Civ. P. 12(h)(3) (providing that courts must dismiss any part of lawsuit over which it lacks subject matter jurisdiction). When assessing Article III standing at

the pleading stage, courts consider whether a plaintiff has "clearly allege[d] facts" that demonstrate the following three elements: (1) the plaintiff has suffered an injury in fact; (2) the claimed injury is "fairly traceable" to the defendant's alleged conduct; and (3) the relief sought will redress the claimed injury. Alleruzzo v. SuperValu, Inc. (In re SuperValu, Inc. Customer Data Sec. Breach Litig.), 870 F.3d 763, 768 (8th Cir. 2017) (quoting Spokeo v. Robins, 578 U.S. 330, 338 (2016)). Horizontal's arguments attacking Devine's Article III standing center on the requirements of injury in fact and traceability. To establish injury in fact, a plaintiff must show that he suffered an injury that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." Spokeo, 578 U.S. at 339. "Concrete" injuries include "traditional tangible harms, such as physical harms and monetary harms," as well as "intangible harms" that are closely related to traditional harms, such as "reputational harms, disclosure of private information, and intrusion upon seclusion." TransUnion LLC v. Ramirez, 594 U.S. 413, 424–25 (2021). "Particularized" injuries must "affect the plaintiff in a personal and individual way." Spokeo, 578 U.S. at 339 (quotation omitted). To establish traceability, "there must be 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 a third party not before the court. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992). "A plaintiff must 'demonstrate standing separately for each form of relief sought.'" TransUnion, 594 U.S. at 436 (quoting Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), 528 U.S. 167, 185 (2000)). Here, Devine seeks both equitable and monetary relief, and the Court addresses each in turn. A. Standing for Equitable Relief Devine seeks injunctive and declaratory relief to require Horizontal to implement an adequate cybersecurity system and policies to protect and safeguard his PII/PHI from future breaches of Horizontal's computer systems. (Am. Compl. at 34; see id. ¶¶ 55, 155–57.) The Court concludes that Devine has not made sufficient allegations to support the requests for injunctive and declaratory relief. When a plaintiff seeks equitable relief to prevent future harm from occurring, concrete injuries can include "the risk of real harm," so long as the risk is "sufficiently imminent and substantial." TransUnion, 594 U.S. at 435–36. However, "[t]he universal interest in the security of one's private data does not equate to a substantial and imminent risk of harm." Thomas v. Pawn Am. Minn., LLC (In re Pawn), No. 21-CV-2554 (PJS/JFD), 2022 WL 3159874, at *3 (D. Minn. Aug. 8, 2022). In this case, to justify the injunctive and declaratory relief requested, the allegations in the Amended Complaint must establish a likelihood that Horizontal will experience a future breach. The allegations in the Amended Complaint, however, do not adequately address whether Horizontal is likely to experience a future data breach, and are therefore insufficient to state an imminent and substantial risk. For example, the Amended Complaint includes conclusory speculations that cybercriminals could "perpetuate new data breaches" because the unencrypted passwords and login credentials of Horizontal employees are on the "dark web." (Am. Compl. ¶ 22.)2 Similarly, the Amended Complaint includes allegations that Device faces "continued risk to [his] PII/PHI—which remains in

[Horizontal]'s possession—and is thus at risk for future breaches so long as [Horizontal] fails to take appropriate measures to protect the PII/PHI." (Id. ¶ 56.h.) The Amended Complaint also references a list of the Federal Trade Commission guidelines on best data security practices, industry standard best practices, and safeguards mandated by the Health Insurance Portability and Accountability Act (HIPPA). (Id. ¶¶ 69–74, 75–78, 79–82.) However, he alleges only that Horizontal failed to implement these measures before the Data Breach. (Id.) Without more, these allegations do not establish a "certainly impending" or "substantial risk" that Horizontal will experience a future breach absent the injunctive and declaratory relief sought. Instead, as another court has observed, Horizontal "faces much the same risk of future cyberhacking as virtually every holder of private data." 2 In his opposition brief, Devine also concedes that the encrypted passwords referred to in the Amended Complaint were present on the dark web before the Data Breach. (Doc. No. 25 at 3 (citing Am. Compl. ¶ 22).) Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 378 (1st Cir. 2023). "If that risk were deemed sufficiently imminent to justify injunctive relief, virtually every company and government agency might be exposed to requests for injunctive relief like the one the plaintiffs seek here." Id. Because Devine has not demonstrated standing for the requested equitable relief, the Court must dismiss these requests. B. Standing for Monetary Relief Devine also seeks monetary damages flowing from Horizontal's conduct. In suits for damages, "the mere risk of future harm, standing alone, cannot qualify as a concrete harm . . . unless the exposure to the risk of future harm itself causes a separate concrete harm." TransUnion, 594 U.S. at 436. Under this portion of the analysis, the focus shifts from harm that Devine might suffer from future breaches of Horizontal's computer systems to harm that Devine has suffered or will likely suffer because of the data breach that already occurred. See Pawn, 2022 WL 3159874, at *9. The Amended Complaint includes allegations regarding seven separate categories of harm stemming from the Data Breach. The Court addresses each category in turn and concludes that the allegations are insufficient to establish any concrete injury.

1. Disclosure of Private Information

Devine argues that he has suffered a concrete injury because his PII/PHI was disclosed as a result of the Data Breach. (Doc. No. 25 at 8–11.) While "disclosure of private information" constitutes a concrete injury, see TransUnion, 594 U.S. at 424–25, Devine's argument mischaracterizes the allegations in the Amended Complaint, which do not identify any of Devine's PII/PHI that was disclosed. The Amended Complaint includes general allegations concerning the types of data that were potentially disclosed for some of Horizontal's current and former employees, including Devine. (Am. Compl. ¶¶ 19–20.) In addition, the Amended Complaint includes a reference to the Notice of the data breach. (Id. ¶¶ 18–19.) This Notice appears to warn individuals that their "information was present in" certain files that were accessed or taken from Horizontal's system and that those files may have contained their unspecified "personal information." Id. The Notice also indicates that Horizontal was still investigating the "nature and scope" of the Data Breach. Id. Devine alleges that the Notice shows that Horizontal either cannot or will not determine the full

scope of the Data Breach because it "has been unable to determine precisely what information was stolen and when." (Am. Comp. ¶ 29.) He also links a data security breach report from the Texas Attorney General's Office, which shows that the "type(s) of information affected" included names, social security numbers, driver's license numbers, financial information (e.g., account number, credit or debit card number), and medical information. (Id. ¶ 20 n.13 (linking Texas Data Breach).) These portions of the Amended Complaint, however, fail to clearly allege facts that demonstrate what of Devine's own information was accessed or taken in the Data Breach. Absent any allegations concerning his own PII/PHI, Devine has not alleged any concrete or particularized harm from his alleged loss of privacy. He therefore cannot establish standing on this basis. To convince the Court otherwise, Devine cites to Perry v. Bay & Bay Transp. Servs., Inc., 650 F. Supp. 3d 743, 752 (D. Minn. 2023) and Pawn, 2022 WL 3159874, at *4. . Both cases are readily distinguishable. In Perry, the plaintiff identified his own private information that he alleged had been disclosed to cybercriminals. Perry, 650 F. Supp. 3d at 749. Similarly, at least some of the plaintiffs in Pawn alleged disclosure of their private information. 2022 WL 3159874, at *4. Contrary to Devine's argument, both Perry and Pawn involved specific allegations that are absent from the Amended Complaint.

2. Imminent and Substantial Risk of Identity Theft Stemming from the

Disclosure of Devine's Private Information Devine also argues that the Amended Complaint states a concrete injury of future risk of identity theft because his PII/PHI was disclosed. This argument also mischaracterizes the actual allegations in the Amended Complaint, which do not adequately allege any future risk of identity theft as a result of the Data Breach. First, as noted above, the Amended Complaint does not adequately allege what information about Devine was disclosed. Without such allegations, the Amended Complaint cannot adequately tie future harm to the disclosure of Devine's own PII/PHI. Second, even assuming that the Amended Complaint did specify what of Devine's PII/PHI had actually been disclosed in the Data Breach, the Amended Complaint includes no allegations that Devine's unique PII/PHI has been affected by the breach, that his PII/PHI has been misused in any way, or that he has experienced any concrete or particularized injury resulting from the alleged disclosure of his own PII/PHI. Again, the factual allegations in Perry and Pawn go well beyond those in this case. The plaintiff in Perry alleged that cybercriminals misused his specific private information that had been disclosed in the data breach to contact him, impersonate his bank, and scam him out of $500. Perry, 650 F. Supp. 3d at 749. Likewise, at least some of the plaintiffs in Pawn alleged that as a direct result of the disclosure of their private data, they experienced identify theft. 2022 WL 3159874, at *4. Thus, Devine has not pleaded facts to show that a sufficient risk of future harm has materialized. See TransUnion, 594 U.S. at 437.

3. Separate Concrete Harms Stemming from PII/PHI Disclosure: Time,

Effort, and Costs Incurred Devine next argues that his exposure to the risk of future harm caused him to expend time and effort monitoring his accounts and credit reports and sorting through a

substantial increase in spam. (Doc. No. 25 at 11–12; Am. Compl. ¶¶ 44, 56, 114, 176.) Devine also "anticipates spending considerable amounts of time and money to try and mitigate his injuries." (Am. Compl. ¶ 51.) Absent allegations that his own PII/PHI was disclosed, however, the Amended Complaint contains insufficient allegations to state an injury stemming from the time, effort, and money that Devine expended to monitor his accounts. A plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013). If "plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury." SuperValu, 870 F.3d at 771. As discussed above, Devine has not established that he faces a substantial and imminent risk of harm. Consequently, any time, effort, or costs that he has spent has been in response to a purely speculative threat. Again, Devine urges the Court to reach a different conclusion but relies on readily distinguishable legal authority. Devine directs the Court's attention to the reasoning in Webb, which concluded 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." 72 F.4th at 376–77. Webb, however, undermines Devine's position because the plaintiffs in Webb alleged actual misuse of PII resulting from a data breach—specifically, some of the stolen PII had been misused to file a fraudulent tax return in Webb's name. Id. at 377. Because of these specific allegations, which the First Circuit determined were a substantial and imminent risk of harm, the plaintiffs had adequately pleaded a plausible injury due to lost time that resulted from the filing of the fraudulent tax return. In contrast to the allegations in Webb, as noted above, the Amended Complaint includes no allegations of any actual misuse of Devine's PII/PHI—nor does he plausibly allege a material risk of future misuse. Because Devine has not alleged that his PII/PHI has been used by anyone in a way that could create a substantial risk of future identity theft, he fails to establish standing on the basis of time, effort, and costs incurred to monitor his bank accounts and credit reports.

4. Spike in Spam Emails

Devine also alleges that "in the aftermath of the Data Breach, [he] has suffered from a spike in spam and scam emails." (Am. Compl. ¶ 45.) The Court concludes that the Amended Complaint does not plausibly plead allegations to establish that "a spike in spam and scam emails" was traceable to the Data Breach. As a threshold matter, the Court observes that some "[c]ourts in the Eighth Circuit have . . . found increased spam . . . can qualify as an injury in a data breach case." Berry v. Crescent Cmty. Health Ctr., No. 24-CV-1036 (CJW/KEM), 2025 WL 1287909, at *5 (N.D. Iowa May 2, 2025) (citing cases and finding that plaintiff allegation of increased spam calls constituted an injury). Courts in other districts, however, have rejected this theory. See, e.g., Blood v. Labette Cnty. Med. Ctr., No. 5:22-CV-4036 (HLT/KGG), 2022 WL 11745549, at *6 (D. Kan. Oct. 20, 2022) ("[T]he alleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact."); Legg v. Leaders Life Ins. Co., 574 F. Supp. 985, 993 (W.D.

Okla. 2021) ("[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." (quotation omitted)); In re Practicefirst Data Breach Litig., No. 1:21-CV-00790 (JLS/MJR), 2022 WL 354544, at *5 n.8 (W.D.N.Y. Feb. 2, 2022), report and recommendation adopted, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 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"). The Court need not determine whether "a spike in spam emails" constitutes an injury in fact, because, in this case, the Amended Complaint fails to plausibly plead traceability. Courts have found that "simply alleg[ing] that [an] [injury] happened after the . . . breach" does not "sufficiently connect" the Data Breach to the injury. Welborn v. Internal Revenue Servs., 218 F. Supp. 3d 64, 79 (D.C.C. 2016) (concluding that plaintiff did not show that her injury was fairly traceable to data breach where she alleged that she was only ever notified of one breach and she had been the victim of "at least two occasions of fraudulent activity in her financial accounts, one of which resulted in the removal of funds from a personal financial account, which occurred after the . . . breach" (internal quotation marks omitted)); see also McCombs v. Delta Grp. Elec., Inc., 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023) ("Spam calls, texts, and e-mails have become very common in this digitized world, and a number of courts have declined to confer standing when considering an increase in spam communications." (citing cases)). In this case, the Amended Complaint contains no allegations that his email address was disclosed or stolen in the Data Breach. Indeed, the allegations do not specify any types of information that Horizontal identified as stolen in its notices of the data breach because the notices themselves did not specify such information. In addition, none of the allegations describe the subject matter of the emails, so it is impossible to determine whether the emails were related to the Data Breach. Moreover, the Amended Complaint includes only one allegation concerning the timing of the increased spam and scam communications: they occurred "in the aftermath of the Data Breach." (Am. Compl. ¶ 45.) Such allegations are insufficient to show traceability as required to establish standing for recovering damages for increased spam and scam communications.

5. Harm to Credit

The Amended Complaint also includes allegations that Devine's credit report was negatively impacted. The Court concludes, however, that these allegations fail to establish the necessary connection to the Data Breach to show traceability. The factual allegations in the Amended Complaint state that "shortly after" the Data Breach, Devine received an email from someone who "purported to be Experian" and "claimed that his credit report had been subject to an excessive amount of inquiries," which he does not recall authorizing. (Am. Compl. ¶ 52.) Devine also alleges that "following" the Data Breach, he "discovered his credit score had dropped to . . . a number Plaintiff believes to be lower than what it had been" before the Data Breach. (Id. ¶ 53.) These alleged injuries are not "fairly traceable" to the Data Breach, as opposed to "the result of the

independent action of some third party not before the court." Lujan, 504 U.S. at 560. The fact that these events happened "following" the Data Breach does not adequately link them to the Data Breach. Credit scores can lower for a variety of reasons, and credit reports can be subject to inquiries for a variety of reasons. Although harm to credit may be a cognizable injury, Devine has not established that any alleged harm to his credit is fairly traceable to the Data Breach.

6. Diminished Value of PII/PHI and Lost Benefit of the Bargain

Devine alleges a diminution of value in his PII/PHI as well as "lost benefit of their bargain." (Am. Compl. ¶¶ 49, 114.) These allegations, however, are too general and conclusory to plausibly plead an injury in fact. For instance, the allegations do not purport to state what the monetary value was of Devine's PII/PHI or, as noted above, even identify what specific PII/PHI was disclosed.3 In addition, even if the Amended Complaint included allegations to plausibly plead that his specific PII/PHI was disclosed and that it had monetary value, the Amended Complaint does not contain any factual allegations explaining how the monetary value was reduced or diminished as a result of the Data Breach. For example, there are no allegations that Devine tried to sell his PII/PHI and was forced to accept less as a result of the Data Breach. See Blood v. Labette Cnty. Med. Ctr., No. 5:22-CV-04036-HLT-KGG, 2022 WL 11745549 (D. Kan. Oct. 20, 2022); Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564, 572 (D. Md. 2016). The Court, therefore, concludes that the Amended Complaint fails to allege an injury based on diminution in value of his PII/PHI.

7. Emotional Distress

Finally, the Amended Complaint includes allegations that Devine experienced emotional injury. These allegations, however, are not fairly traceable to the Data Breach, 3 To the extent that Devine asserts a "lost benefit of their bargain" as a separate category of injury from the diminution of value in his PII/PHI, the Court concludes that the Amended Complaint contains insufficient allegations to establish an injury in fact. The cases cited by Devine to support such an injury are factually dissimilar from the facts here because, contrary to the factual allegations in this case, in the cases relied on by Devine the plaintiffs alleged actual misuse of their private information following a data breach. See Priddy v. Zoll. Med. Corp., No. 1:23-CV-10575-IT, 2025 LEXIS 62112, at *26 (D. Mass. Mar. 31, 2025); In re Marriott Int'l, Inc., 440 F. Supp. 3d 447, 462–65 (D. Md. 2020); Plaintiffs v. MGM Resorts Int'l, 638 F. Supp. 3d 1175, 1186 (D. Nev. 2022). Here, Devine has not alleged any misuse of his or any other employee's PII/PHI. Furthermore, as discussed above, the Amended Complaint does not allege that his PII/PHI was of any material economic value with respect to any service he received from Horizontal. See In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2904, 2021 WL 5937742, at *11 (D.N.J. Dec. 16, 2021). Thus, Devine lacks standing to assert a claim based on a theory that the Data Breach resulted in a lost benefit of the bargain. absent additional allegations that Devine's own PII/PHI was disclosed, and allegations that it was this disclosure that caused the emotional distress. A plaintiff's knowledge of their exposure to "a risk of future physical, monetary, or reputational harm" could cause the plaintiff to suffer "emotional or psychological harm."

TransUnion, 594 U.S. at 436 n.7. Such emotional or psychological harm, however, must be sufficiently connected to an actual disclosure of information to establish standing. See SuperValu, 870 F.3d at 771 (concluding that because the plaintiffs "have not alleged a substantial risk of future identity theft," they lacked standing to seek relief for injuries created by "this speculative threat" of future identity theft); see also Clapper, 568 U.S. at 416 (concluding that a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending"); Pawn, 2022 WL 3159874, at *4 (concluding that allegations of emotional distress directly caused by the theft of plaintiffs' private information were sufficient to establish standing because "at least some plaintiffs ha[d] alleged that their identities ha[d] already been stolen because of the data breach"). In this case, as noted above, the Amended Complaint does not contain allegations that Devine's own PII/PHI was disclosed or that Devine faces a substantial risk of identity theft stemming from the disclosure of his PII/PHI. While the Amended Complaint alleges that Devine experienced "anxiety, sleep disruption, stress, fear, and frustration," that "go beyond allegations of mere worry or inconvenience," because of his fear about "his personal financial security" and about "what information was exposed in the Data Breach" (Am. Compl. ¶¶ 46–47), these fears are not plausibly traceable to the Data Breach absent allegations of actual disclosure and actual misuse of Devine's own PII/PHI. Therefore, the Amended Complaint does not establish standing for a claim of emotional distress. In sum, Devine has not demonstrated standing for his request for monetary relief, and the Court dismisses this request for lack of jurisdiction.4

ORDER

Based on the foregoing, and on all of the files, records, and proceedings herein, IT IS HEREBY ORDERED THAT Defendant's Motion to Dismiss (Doc. No. 14) is GRANTED WITHOUT PREJUDICE. LET JUDGMENT BE ENTERED ACCORDINGLY. Dated: December 19, 2025 /s/ Jeffrey M. Bryan Judge Jeffrey M. Bryan United States District Court 4 Because the Court concludes that Devine lacks standing, it need not address whether Devine has failed to state a claim under Rule 12(b)(6).