WESTIN THE UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

Case No. 23-cv-00586-MEH

PAULA HENDERSON,
SHYKIRA SCOTT,
DANIEL JONES,
CAROL GOLDBERG,
VAHRAM HAROUTUNIAN,
BRIAN KEARNEY,
HILDA LOPEZ,
PREFERENCE ROBINSON,
SHARON ETCHIESON,
RADHE BANKS,
JONATHAN TRUSTY,
MARIE NETROSIO,
MICHAELA MUJICA-STEINER,
ROGER LOEB, and
KYLE DENLINGER, *on behalf of themselves and all others similarly situated*,

Plaintiffs,

v.

REVENTICS, LLC, and
OMH HEALTHEDGE HOLDINGS, INC., d/b/a Omega Healthcare,

Defendants.

ORDER

Michael E. Hegarty, Chief United States Magistrate Judge.

Plaintiffs—fifteen named individuals from seven, consolidated putative class action lawsuits—assert claims against Defendants Reventics, LLC and OMH Healthedge Holdings, Inc. ("Omega"), stemming from a 2022 data breach of Reventics's computer systems. Defendants have filed a Motion to Dismiss, seeking dismissal of this case in its entirety under Federal Rules

of Civil Procedure 12(b)(1) and 12(b)(6). ECF 64.[1] The Motion is fully briefed, and oral argument would not materially assist the Court in its adjudication. For the foregoing reasons, the Court concludes that Plaintiffs do not have Article III standing and grants Defendants' Motion.

FACTUAL BACKGROUND

For the purposes of ruling on Defendants' Motion to Dismiss, the Court accepts as true the factual allegations—as opposed to any legal conclusions, bare assertions, or conclusory allegations—that Plaintiffs raise in their Second Amended Consolidated Complaint. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

Defendants in this case are healthcare software companies. Generally, Reventics provides software "to improve clinical documentation and revenue cycle management." ECF 39 ¶ 30. To do so, Reventics collects patient data from physicians, translates the items in a patient's chart into billing codes for submission to insurance companies, and generates and submits payment requests. *Id.* at ¶¶ 30–35. Reventics further uses patient data to build analytical models related to insurance claim payment metrics. *Id.* ¶ 35. Through this work, Reventics requests and stores personally identifiable information ("PII") and protected health information ("PHI"), such as first, middle, and last name, address, date of birth, Social Security number, diagnosis information, prescription medications, symptoms, and dates of service. *Id.* ¶¶ 1, 35. Omega offers software and support services to physicians through a network of various healthcare services companies that Omega

[1] While Defendants' Motion is filed on the docket at ECF 64, this filing is simply a two-page summary of Defendants' position. Defendants separately filed a Memorandum in support of the Motion at ECF 65 which contain Defendants' full arguments and citations to legal authority. In the interests of judicial economy, the Court will consider the arguments proffered in Defendants' separate Memorandum, however the Court notes that pursuant to Local Rule of Civil Practice 7.1, "a motion involving a contested issue of law shall state under which rule or statute it is filed and be supported by a recitation of legal authority *in the motion*." D.C.COLO.LCivR 7.1(d) (emphasis added).

owns, controls, or otherwise maintains. *Id.* ¶ 38. Omega acquired Reventics in March 2022, and integrated Reventics's software platforms into its network of other entities to deliver "end-to-end revenue cycle management" for healthcare providers. *Id.* ¶ 40. Omega also offers software and backend office support to help physicians work with Medicare patients, secure approval for medications, and manage clinical research. *Id*. ¶¶ 47–49. Through its work, Omega collects and maintains patient PHI/PII. *Id.* ¶ 45.

On December 15, 2022, Reventics discovered that cyber criminals had accessed and encrypted its network. *Id.* ¶ 52. Approximately two weeks later, on December 27, 2022, a cybersecurity firm determined cybercriminals had exfiltrated patients' PHI/PII from Reventics servers, including names, dates of birth, Social Security numbers, and clinical data. *Id.* ¶ 53. On February 10, 2023, Reventics reported that cybercriminals accessed over 250,000 patient records. *Id.* ¶¶ 4, 54. Beginning in February 2023, Defendants began disseminating a "Notice of Data Security Incident" reporting the breach to state Attorneys General and impacted individuals. *Id.* ¶¶ 4, 59. The notice admits that unauthorized acquisition of information occurred on or about December 27, 2022, and lists the categories of PHI/PII that were impacted by the breach. *Id.* ¶¶ 61, 62. Several waves of the notice have been issued as Defendants uncovered the identities of additional people affected by the breach. *Id.* ¶ 63.

Plaintiffs are all individuals who provided their PHI/PII to various medical providers who, in turn, provided it to Defendants. *Id.* ¶ 94. Defendants' Notice of Data Security Incident notified Plaintiffs their PHI/PII may have been involved in the data breach. *Id.* ¶ 99. Following receipt of the notice, Plaintiffs allege they suffered actual injuries in the form of time spent self-monitoring their accounts; diminution of the value of their PHI/PII; and lost time, annoyance, and inconvenience. *Id.* ¶¶ 101–104. They also report that since the time of the data breach, they have

received increased spam communications, including emails or phone calls. *Id.* ¶¶ 115, 122, 128, 136, 151. Plaintiffs also allege future injury "from the present and ongoing risk of fraud, identity theft and misuse" of their PHI/PII. *Id.* ¶ 105.

Some of the Plaintiffs allege additional injuries to those noted above. Paula Henderson claims that "[f]ollowing the Data Breach, [she] experiences fraudulent charges on her debit card and had to replace her debit card." *Id.* ¶ 110. Sharon Etchieson alleges she placed freezes on her account following receipt of Defendants' Notice of Data Security Incident and her approval for a loan was delayed "by weeks" due to the credit freezes on her accounts. *Id.* ¶ 115. Brian Kearney alleges that in March 2023, he received a notice that an unknown person had attempted to open a credit card in his name through Bank of America. *Id.* ¶ 143. Finally, Plaintiff Preference Robinson claims that in February 2023, a fraudulent cell phone account was established in her name. *Id.* ¶ 158.

LEGAL STANDARDS

I. Fed. R. Civ. P. 12(b)(1)

Federal courts are courts of limited jurisdiction and, as such, "are duty bound to examine facts and law in every lawsuit before them to ensure that they possess subject matter jurisdiction." *The Wilderness Soc. v. Kane Cty.*, Utah, 632 F.3d 1162, 1179 n.3 (10th Cir. 2011) (Gorsuch, J., concurring). Indeed, courts have an independent obligation to determine whether subject matter jurisdiction exists, even in the absence of a challenge from any party. *1mage Software, Inc. v. Reynolds & Reynolds, Co.*, 459 F.3d 1044, 1048 (10th Cir. 2006) (citing *Arbaugh v. Y & H Corp.*, 546 U.S. 500 (2006)).

Pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure, a party may bring either a facial or factual attack on subject matter jurisdiction, and a court must dismiss a complaint if it

lacks subject matter jurisdiction. *See generally Pueblo of Jemez v. United States*, 790 F.3d 1143, 1147 n.4 (10th Cir. 2015). For a facial attack, the court takes the allegations in the Complaint as true; however, when reviewing a factual attack, the court may not presume the truthfulness of the Complaint's factual allegations and may consider affidavits or other documents to resolve jurisdictional facts. *Holt v. United States*, 46 F.3d 1000, 1002-03 (10th Cir. 1995). The burden of establishing jurisdiction rests with the party asserting jurisdiction. *Basso v. Utah Power & Light Co.*, 495 F.2d 906, 909 (10th Cir. 1974).

II. Fed. R. Civ. P. 12(b)(6)

The purpose of a motion to dismiss under Fed. R. Civ. P. 12(b)(6) is to test the sufficiency of the plaintiff's complaint. *See Sutton v. Utah State Sch. for the Deaf & Blind*, 173 F.3d 1226, 1236 (10th Cir. 2008). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

Twombly requires a two-prong analysis. *Id.* at 678. First, courts must identify "the allegations in the complaint that are not entitled to the assumption of truth," that is, those allegations which are "legal conclusions," "bare assertions," or merely "conclusory." *Iqbal*, 556 U.S. at 678, 680–81. Indeed, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678 (citing *Twombly*, 550 U.S. at 555). Second, courts must consider the factual allegations "to determine if they plausibly suggest an entitlement to relief." *Id.* at 681. Plausibility, in the context of a motion to dismiss, means that the plaintiff pleaded facts which "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678 (citing *Twombly*, 550 U.S. at 556). "The nature and specificity of the allegations required to state a plausible claim will vary based on context." *Safe*

Streets All. v. Hickenlooper, 859 F.3d 865, 878 (10th Cir. 2017) (quoting *Kan. Penn Gaming, LLC v. Collins*, 656 F.3d 1210, 1215 (10th Cir. 2011)). Thus, "[w]hile the 12(b)(6) standard does not require that [a plaintiff] establish a prima facie case in [a] complaint, the elements of each alleged cause of action may help to determine whether [a plaintiff] has set forth a plausible claim." *Khalik*, 671 F.3d at 1191 (internal citations omitted).

ANALYSIS

I. Article III Standing

This case wades into the muddy waters that is Article III standing in the context of data breach cases. Article III of the United States Constitution limits federal courts' jurisdiction to "cases" and "controversies." *E.g., Lujan v. Defs. of Wildlife,* 504 U.S. 555, 560 (1992). To present a case or controversy under Article III, a plaintiff must establish that he has standing to sue. *Id.* Courts have an independent responsibility to examine subject matter jurisdiction, *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94–95 (1998) and must dismiss the action if subject matter jurisdiction is lacking. Fed. R. Civ. P. 12(h)(3) ("If the court determines at any time that it lacks subject-matter jurisdiction, the court must dismiss the action.").

Article III's standing analysis requires three things: the plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citing *Lujan,* 504 U.S. at 560–61). Plaintiffs "bear[] the burden of establishing these elements," which, at this stage of the case, requires they "allege facts demonstrating each element." *Id.* Defendants argue most of the named Plaintiffs fail to allege an injury in fact—the

first element of Article III standing. ECF 65 at 15–18.[2] They further contend that the Plaintiffs who do allege a specific and actual injury in fact fail to plausibly allege that the purported injury is traceable to the data breach—the second element of standing. *Id.* at 18–20. Finally, they argue none of the Plaintiffs have standing to seek declaratory or injunctive relief. *Id.* at 20–21. In light of Defendants' arguments, the Court focuses its analysis on the first two elements of standing—an injury in fact and a causal connection.

To show the first element of standing—injury in fact—a plaintiff must demonstrate he suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *See Lujan*, 504 U.S. at 560. "A 'concrete' injury must be 'de facto'; that is, it must actually exist." *Spokeo, Inc.*, 136 U.S. at 340. To be "imminent," a "threatened injury must be *certainly impending* to constitute injury in fact" and "allegations of *possible* future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (cleaned up) (emphasis in original). While there can be a "substantial risk" that the harm will occur, *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014), mere risk of future harm without more is insufficient to confer standing. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 434–436 (2021).

For the second element of standing—that the injury is "fairly traceable" to the challenged conduct—a plaintiff must allege "a substantial likelihood that the defendant's conduct caused plaintiff's injury in fact." *Nova Health Sys. v. Gandy,* 416 F.3d 1149, 1156 (10th Cir. 2005). The plaintiff must "establish that its injury was not the result of the independent action of some third party not before the court." *Santa Fe All. for Pub. Health & Safety v. City of Santa Fe, N.M.*, 993

[2] The Court cites to the CM/ECF document number and page in the CM/ECF heading at the top of the Parties' briefing rather than to the documents' page numbers at the bottom of each page.

F.3d 802, 814 (10th Cir. 2021) (quotation omitted). A plaintiff must allege more than a "speculative chain of possibilities," *Clapper*, 568 U.S. at 414, and must advance allegations that, if true, show the defendant's conduct is a "but for" cause of the injury. *Santa Fe All. for Pub. Health & Safety*, 993 F.3d at 814.

II. Standing in Data Breach Cases

Upon even just a quick survey of relevant cases, it is clear that data breach litigation presents "unique and modern issues related to standing." *McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1070 (D.N.M. 2023). The current state of the caselaw is such that some circuits have concluded that data breach victims have sustained an injury in fact based on the underlying disclosure of their personal information to hackers. *See C.C. v. Med-Data Inc.*, No. 21-cv-2301, 2022 WL 970862, at *3 (D. Kan. Mar. 31, 2022) (collecting cases); *e.g., Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 691–95 (7th Cir. 2015) ("[C]ustomers 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." (quotation omitted)); *see also 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"). As noted by other courts, however, these cases generally have included allegations of actual misuse of the leaked data. *McCombs*, 676 F. Supp. 3d at 1070.

Conversely, other circuits—including the Second, Third, Eighth, and Eleventh—have concluded that data breach victims do not sustain an injury in fact merely because of the data breach alone, where the plaintiffs rely on the inherent harm of unauthorized access to their PII to

make their claims. *See Med-Data Inc.*, 2022 WL 970862, at *3 (collecting cases). Since 2013, "a majority of the lower federal courts addressing 'lost data' or potential identity theft cases in which there is no proof of actual misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data." *McCombs*, 676 F. Supp. 3d at 1070 (quoting Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits*, 92 Notre Dame L. Rev. 1323, 1324 (2017)).

To date, the Tenth Circuit has yet to weigh in on this issue. However, a number of other districts courts in this Circuit have addressed standing in data breach cases. *E.g., Blood v. Labette Cnty. Med. Ctr.*, No. 22-cv-04036, 2022 WL 11745549, at *3 (D. Kan. Oct. 20, 2022); *McCombs*, 676 F. Supp. 3d at 1070; *Med-Data Inc.*, 2022 WL 970862, at *3; *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 988 (W.D. Okla. 2021). These sister districts have all followed the view that a plaintiff does not suffer an injury in fact where their PII is accessed through a data breach but no direct harm results. This Court is persuaded to follow the same reasoning.

III. Plaintiffs' Alleged Injuries

Plaintiffs argue they have suffered six forms of injury sufficient to confer Article III standing in this case: (1) public disclosure of private information, including Social Security numbers and medical information; (2) increased spam communications; (3) diminution of the value of their PHI/PII; (4) emotional distress; (5) actual fraud; and (6) "future impending injury." ECF 86 at 15.[3] The Court addresses each category in turn.

[3] To the extent Plaintiffs attempt to claim they were injured by Defendants' violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), or various state consumer protection act statutes, their allegations fail to establish standing because violation of the law does not establish standing absent injury in fact. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) ("Standing . . . does not merely require a showing that the law has been violated, or that a statute will reward litigants in general upon showing of a violation.").

A. Public Disclosure of Private Information

Plaintiffs first contend the mere fact that their private information was publicly disclosed through the breach (without more) is enough to plead an injury in fact. ECF 86 at 15. As noted above, most courts to consider this issue agree the mere loss of data—without allegations that the data has been misused—does not constitute an injury in fact sufficient to confer standing. *E.g.*, *Chambliss v. Carefirst, Inc*, 189 F. Supp. 3d 564, 571 (D. Md. 2016) (collecting cases). Indeed, since the Supreme Court's decision in *Clapper v. Amnesty International*—in which the Court held that injuries that are not "certainly impending" cannot confer standing, 568 U.S. at 410—courts "have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases." *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28 (D.D.C. 2014). Thus, the mere fact that Plaintiffs' data was compromised in the breach does not confer them standing in this case.

Plaintiffs also allege that because their information was compromised through the breach, they suffered an injury in fact based on their costs mitigating the increased risk of identity theft or fraud, specifically time spent monitoring their accounts or credit reports and expenses incurred to obtain credit monitoring services. *E.g.*, ECF 39 ¶¶ 101, 110, 115. Courts have repeatedly rejected the argument that such costs constitute injuries in fact as they are costs incurred due to a plaintiff's own apprehension of speculative future harms. *E.g.*, *McCombs*, 676 F. Supp. 3d at 1073; *Blood*, 2022 WL 11745549, at *6; *Masterson v. IMA Fin. Grp., Inc.*, No. 23-cv-02223, 2023 WL 8647157, at *6 (D. Kan. Dec. 14, 2023) ("Actions taken based on a hypothetical future threat does not create a concrete injury.") (collecting cases); *Chambliss*, 189 F. Supp. 3d at 571 ("In the context of data breach litigation, courts have consistently held that a plaintiff may not use mitigation costs alone to establish a cognizable injury in fact."). Plaintiffs "cannot manufacture

standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 402 (2013). Stated differently, "while 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." *Legg*, 2021 WL 5772496, at *7. Thus, Plaintiffs' mitigation costs to proactively monitor their credit accounts is not an injury in fact that confers standing.

Plaintiffs also assert a generalized claim they "loss of the benefit of their bargain" due to public disclosure of their information. ECF 39 at ¶¶ 4, 68. These conclusory allegations do not confer standing on Plaintiffs. First, it is unclear to what alleged bargain Plaintiffs are referring. Per their allegations, Plaintiffs provided their PHI/PII to medical providers who then provided this information to Defendants. *Id.* ¶ 94. Plaintiffs do not allege a contractual relationship with Defendants or otherwise elaborate on what is the purported bargain. Second, Plaintiffs fail to explain what is the alleged benefit of that bargain, let alone how the data breach caused them to lose that benefit. Cases considering more elaborate "benefit of the bargain" arguments in data breach cases have found them unavailing. *Med-Data Inc.*, 2022 WL 970862, at *9; *Legg*, 2021 WL 5772496, at *7; *Chambliss*, 189 F. Supp. 3d at 572 (finding that "Plaintiffs have not alleged any benefit-of-the-bargain loss that could constitute a cognizable injury in fact."); *In re Practicefirst Data Breach Litig.*, No. 21-cv-00790, 2022 WL 354544, at *8 n.11 (W.D.N.Y. Feb. 2, 2022) ("The Court also rejects any attempt by plaintiffs to establish standing by alleging that they failed to receive the 'benefit of their bargain' by providing their private information to their medical providers, who then entrusted the data to defendants.") (collecting cases). Consistent with these decisions, the Court finds Plaintiffs' conclusory allegations to be similarly insufficient here.

B. Increased Spam

Courts have found that allegations of increased spam communications, such as calls and emails, after an alleged data breach do not constitute an injury in fact. *E.g., Blood*, 2022 WL 11745549, at *6 (reasoning "[t]he alleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact"); *McCombs*, 676 F. Supp. 3d at 1074 (collecting cases finding that increased spam communications following a data breach do not constitute an injury in fact); *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *5 n.8 (W.D.N.Y. 2022) (same).

Moreover, even if they did, Plaintiff's allegations do not plausibly allege that the underlying data breach was a "but for" cause of the spam communications they received. *Santa Fe All. for Pub. Health & Safety*, 993 F.3d at 814. Plaintiffs assert only generalized claims that "[f]ollowing the Data Breach," or "since the time of the Data Breach," they received an increase in spam messages. ECF 39 ¶¶ 115, 122, 128, 136, 151. First, for the Plaintiffs who allege receiving such communications, there are no allegations that their email addresses or phone numbers were included in their PHI/PII compromised through the breach. *Id.* ¶¶ 114, 120, 127, 134, 149 (identifying these Plaintiffs' categories of PHI/PII allegedly impacted). Second, there are no specific allegations regarding the timing of these communications from which the Court could infer a causal connection between the breach and the spam. Lastly, the Plaintiffs all allege an *increase* in spam communications—as they were already receiving such communications it is impossible to say that the breach played any role in increasing the amount of spam Plaintiffs were already receiving. *See McCombs*, 676 F. Supp. 3d at 1074 (noting that "[s]pam calls, texts, and e-mails have become very common in this digitized world" such that they do not in and of

themselves indicate an individual's data was misused as a result of a data beach). Thus, Plaintiffs' allegations regarding spam communications fail both the first and second elements of standing.

C. Diminution of the Value of PHI/PII

Similarly to spam communications, Courts that have considered allegations of the "loss in value" of PHI/PII in data breach cases have found this is not an injury in fact sufficient to confer standing. *E.g.*, *Legg*, 574 F. Supp. 3d at 994; *Blood*, 2022 WL 11745549, at *6; *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017) ("Courts have rejected allegations that the diminution in value of personal information can support standing."). This Court agrees. To start, the Court is not convinced PHI/PII has independent monetary value. Even assuming it does, Plaintiffs' conclusory allegations do not plausibly show how they suffered a concrete injury through any loss in value—such as through an inability to sell their personal information or a lower price offered in such a sale. As there is no actual damage to Plaintiffs due to the alleged loss in value in their personal information, this is not an injury in fact sufficient to confer standing. *Masterson*, 2023 WL 8647157, at *7 ("Diminution in the value of Plaintiffs' PII and PHI is not a concrete and particularized injury sufficient to confer standing."); *In re Capital One Consumer Data Security Breach Litig.*, 488 F. Supp. 3d 374, 403-04 (E.D. Va. 2020) (citing similar cases).

D. Emotional Distress

Plaintiffs also claim various forms of emotional distress in relation to the data breach, including annoyance, inconvenience, stress, anxiety, and "fears/concerns" related to the potential unauthorized use of their PHI/PII. *E.g.*, ECF 39 ¶¶ 104, 115, 123. These allegations fail to convey standing for the same reason as Plaintiffs' claims for proactive mitigation costs fail: Plaintiffs' emotional distress is based on hypothetical, future harm that is not certainly impending. Thus, the

conclusory allegations Plaintiffs have experienced various forms of emotional distress do not plead an injury in fact. *E.g.*, *Masterson*, 2023 WL 8647157, at *7 (D. Kan. Dec. 14, 2023); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1052 (N.D. Cal. 2022) (finding claims of stress related to data beach case did not constitute an injury in fact for the purposes of standing); *Holmes v. Elephant Ins. Co.*, No. 22-cv-00487, 2023 WL 4183380, at *5 (E.D. Va. June 26, 2023) ("Emotional distress does not constitute a cognizable injury-in-fact" in data privacy litigation.).

E. Actual Fraud

As noted above, four of the named Plaintiffs—Paula Henderson, Sharon Etchieson, Brian Kearney, and Preference Robinson—make specific allegations that they experienced specific instances of fraud or financial loss because of the data breach. *See* Factual Background, *supra*. Defendants argue that to the extent these instances constitute injuries in fact, Plaintiffs fail to plead facts sufficient to establish that the purported injuries are traceable to the data breach. ECF 65 at 18–20. The Court agrees.

Standing requires a "causal connection" between the injury in fact and the complained of conduct. *Lujan*, 504 U.S. at 560. A plaintiff must allege "a substantial likelihood that the defendant's conduct caused plaintiff's injury in fact," *Nova Health Sys.,* 416 F.3d at 1156, because a defendant is not liable for "independent action of some third party," *Santa Fe All. for Pub. Health & Safety.*, 993 F.3d at 814, or injuries that are "too remote," "purely contingent," or "indirect[ ]." *Holmes v. Sec. Inv. Prot. Corp.*, 503 U.S. 258, 268, 271, 274 (1992). Here, there is not a "substantial likelihood" that each of the alleged instances of actual harm were caused by Defendants' data breach.

Paula Henderson alleges that "[f]ollowing the Data Breach, [she] experiences fraudulent charges on her debit card and had to replace her debit card." ECF 39 ¶ 110. But Ms. Henderson

does not allege her debit card account information was included in her PHI/PII allegedly compromised in the breach, *id.* ¶ 109, nor does she allege how the possession of her PHI/PII that was included in the breach would enable someone to access her debit account. With these shortcomings, Ms. Henderson's debit card charges are not fairly traceable to the breach. *See Blood*, 2022 WL 11745549, at *5 (finding overdraft fees charged on a debit account to not be fairly traceable to the data breach where the plaintiffs "do not plead any facts suggesting how the mere possession of their Social Security numbers and names would enable someone to make unauthorized charges on an existing account"); *In re SAIC*, 45 F. Supp. 3d at 31 (holding claims that "unauthorized charges were made to [plaintiffs'] existing credit cards or debit cards" lacked causation for purposes of standing because the plaintiffs did not "allege[ ] that credit-card, debit-card, or bank-account information was on the stolen tapes"). Additionally, Ms. Henderson makes no allegations as to the timing of when she experienced the fraudulent charges in relation to the data breach. ECF 39 ¶ 110. Her generalized claim that the charges happened sometime "following" the data breach is too speculative to support causation. *See Masterson*, 2023 WL 8647157, at *4.

Sharon Etchieson's allegations of realized harm are also not traceable to Defendants. Ms. Etchieson claims that she placed freezes on her credit accounts following receipt of Defendants' Notice of Data Security Incident and, as a result of the credit freezes, her approval for a loan was delayed "by weeks." ECF 39 ¶ 115. As with the allegations Plaintiffs incurred costs to monitor their credit discussed above, Ms. Etchieson's choice to proactively freeze her credit was an act she elected to do to mitigate against hypothetical future harms. The brief delay of her loan approval was not due to Defendants' conduct, but to Ms. Etchieson's independent mitigation action. *Santa Fe All. for Pub. Health & Safety.*, 993 F.3d at 814 (a defendant is not liable for "independent action

of some third party"). Any harm from the delay was self-inflicted and is not directly attributable to Defendants. *Clapper,* 568 U.S. at 402 (Plaintiffs "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").

Finally, Brian Kearney's and Preference Robinson's claims of misuse of their PHI/PII also fail to adequately allege traceability. Mr. Kearney alleges that in March 2023 an unknown person attempted to open a credit card in his name. ECF 39 ¶ 143. However, he does not allege what PHI/PII was allegedly compromised in the breach, or that it was the kind of information necessary to open a credit card. *Id.* ¶ 142. His general allegation that his personal information was compromised in the data breach, without more, permits only "a speculative chain of possibilities" linking his alleged harm and Defendants' conduct. *Clapper*, 568 U.S. at 414. Thus, his injury is not fairly traceable to the breach. *See Blood*, 2022 WL 11745549, at *5; *In re SAIC*, 45 F. Supp. 3d at 31; *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015) ("Plaintiff's allegations that someone attempted to open a bank account in his name, attempted to log in to his email accounts, and that he received an increased number of email advertisements targeting his medical conditions do not allege injuries in fact fairly traceable to the Data Breach, since Plaintiff has not alleged that bank account information or email addresses were on the stolen backup data tapes."). Ms. Robinson claims that in February 2023, a fraudulent cell phone account was established in her name. ECF 39 ¶ 158. Her allegations are similarly flawed as Mr. Kearney's because she fails to allege that her information compromised in the breach are the same categories of information necessary to open a fraudulent cell phone account. Further, the mere fact that the claimed misuse occurred after the data breach is insufficient to plead a "substantial likelihood" that the data breach caused the misuse. *Masterson*, 2023 WL 8647157, at *4. For these reasons, the Court concludes that the alleged misuse of Paula Henderson, Sharon Etchieson, Brian Kearney,

and Preference Robinson's personal information is not fairly traceable to the data breach and does not confer standing.

F. Future Impending Injury

Finally, Plaintiffs claim they face future *potential* injuries, namely an increased risk for fraud or other forms of identity theft and the possible need to expend additional time in the future on "a variety of prudent actions," such as placing credit freezes or alerts with credit reporting agencies, closing or modifying financial accounts, and monitoring credit reports. ECF 39 ¶¶ 105, 248–50.

Although the caselaw is split as to whether and when the risk of future injury based on stolen personal information constitutes an "injury in fact," this Court agrees with its sister districts in the Tenth Circuit that a plaintiff does not suffer an injury in fact where their PHI/PII is accessed through a data breach but no direct harm results. *E.g.*, *McCombs*, 676 F. Supp. 3d at 1071; *Legg*, 574 F. Supp. 3d at 993; *Blood*, 2022 WL 11745549, at *7; *Med-Data*, 2022 WL 970862, at *4; *Masterson*, 2023 WL 8647157, at *8. Here, as discussed above, Plaintiffs' allegations of harm either do not constitute an injury in fact for purposes of standing or are not fairly traceable to the data breach. Without any actual misuse or direct harm, "the risk of future injury and any related future costs of mitigation are too attenuated to establish standing." *Masterson*, 2023 WL 8647157, at *8; *see also Legg*, 574 F. Supp. 3d at 993 (similar); *Blood*, 2022 WL 11745549, at *8 (concluding plaintiffs' claims for risk of future injury do not constitute an injury in fact where there was "no concrete actions on which to base a conclusion that any threatened harm is 'certainly impending.'").

The Court further notes that Plaintiffs' allegations largely consist of a recitation of the general risks of identity theft, how personal information can be sold on illicit internet sites, and

what "a dishonest person" may do with PHI/PII. ECF 39 ¶¶ 231–254. These claims do not allege any actual, specific risks to Plaintiffs. At best, Plaintiffs have alleged that they could be subject to some form of identity fraud at some unknown, future date. This does not suggest that Plaintiffs face a risk of future injury that is "certainly impending" or substantial. *See Clapper*, 568 U.S. at 409. Moreover, such identity theft or fraud will only occur if unknown third parties undertake a series of acts to publish, buy, sell, and then use Plaintiffs' data to make unauthorized purchases or open fraudulent accounts. "A future risk of injury that relies on this sort of speculation about the decisions of independent actors is not sufficient to establish a concrete injury." *Legg*, 574 F. Supp. 3d at 993.

As Plaintiffs lack Article III standing, the Court does not have subject matter jurisdiction over this case and must dismiss the Complaint. Because Plaintiffs lack standing to assert their claims, the Court will not address Defendants' remaining arguments on failure to state a claim.

CONCLUSION

For these reasons, Plaintiffs have failed to allege injuries in fact that are fairly traceable to the Defendants' complained of conduct. Therefore, Plaintiffs lack Article III standing, and this Court is without subject matter jurisdiction to further adjudicate this case. Defendants' Motion to Dismiss [ECF 64] is **granted**, and the Court dismisses Plaintiffs' claims for lack of jurisdiction.

The Clerk of Court is directed to **close** this case.

DATED this 30th day of September, 2024, at Denver, Colorado.

BY THE COURT:

Michael E. Hegarty

Michael E. Hegarty
Chief United States Magistrate Judge