IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

MARK MASTERSON, individually and on behalf of all others similarly situated, et al., **Plaintiffs,** **v.** **IMA FINANCIAL GROUP, INC.,** **Defendant.**	**Case No. 2:23-cv-02223-HLT-ADM**

MEMORANDUM AND ORDER

This case arises out of a data breach. Plaintiffs Mark Masterson, Jessica Abel, and Jason Zerbe claim that Defendant IMA Financial Group, Inc. obtained and stored sensitive information and failed to adequately protect it, which enabled cybercriminals to access the data. Plaintiffs assert various claims on behalf of a class composed of all those whose information was affected. The claims include negligence, negligence per se, breach of implied contract, unjust enrichment, and invasion of privacy.

IMA moves to dismiss for lack of standing and for failure to state a claim. Doc. 23. The Court finds that Plaintiffs lack standing because Plaintiffs have not identified a sufficiently concrete injury that is traceable to IMA. The Court thus grants the motion to dismiss for lack of subject-matter jurisdiction under Rule 12(b)(1).

I. BACKGROUND[1]

IMA is a financial services company. Doc. 19 at ¶ 2. It stores sensitive Personally Identifiable Information ("PII") and Private Health Information ("PHI") about its consumers. *Id.*

[1] The following facts are taken from the Amended Consolidated Class Action Complaint ("complaint"), Doc. 19.

¶ 3. IMA lost control of that PII and PHI when cybercriminals hacked its computer systems. *Id.* The data breach affected consumers who had no relationship with IMA or who never consented to IMA collecting and storing their PII and PHI. *Id.* ¶¶ 4, 25. IMA had obtained that information from third parties. *Id.* ¶ 5.

IMA advertises that it takes "steps to ensure that [consumers'] information is kept safe from unauthorized access. We may use physical, electronic and procedural safeguards to protect [] private information." *Id.* ¶¶ 5, 23. Plaintiffs allege IMA never implemented the necessary security safeguards. *Id.* ¶ 24. During the data breach, cybercriminals had access to the PII and PHI of at least 48,358 individuals for an unknown length of time. *Id.* ¶ 6. IMA learned of the data breach on October 19, 2022. *Id.* ¶ 32. It did not notify potential victims of the breach until April 19, 2023. *Id.* ¶ 35. After acknowledging the data breach, IMA warned those affected to take certain precautions, such as monitoring credit reports and freezing credit. *Id.* ¶ 38.

Plaintiffs are individuals who received notice that they were victims of the data breach. *Id.* ¶ 8. They bring this class action on behalf of other data-breach victims. *Id.*

Zerbe is a Colorado resident. *Id.* ¶ 10. Zerbe is unsure how IMA got his information, though he assumes it was provided by his employer. *Id.* ¶ 27.

Masterson is a Kansas resident. *Id.* ¶ 11. Masterson is unsure how IMA got his information, though he assumes it was provided by his employer. *Id.* ¶ 28. In September 2023, Masterson detected some unauthorized charges on his Medicare explanation of benefits. *Id.* ¶ 57. The charges were for medical services he never received, and which occurred in May and June 2023—after the data breach. *Id.* ¶ 57. Masterson has also received a call from an unknown party who had some of his personal information and was offering him a "Medicare benefit." *Id.* ¶ 58. His physician received a similar call, which resulted in another unauthorized charge. *Id.*

Abel is a Kansas resident. *Id.* ¶ 12. Abel is unsure how IMA got her information, though she assumes it was provided by her employer. *Id.* ¶ 29. In January and June 2023, Abel had several instances of unauthorized charges to her credit and debit cards. *Id.* ¶ 69.

Zerbe, Masterson, and Abel have spent time monitoring their accounts, fear for their personal financial security, *id.* ¶¶ 47-48, 59-60, 70-71, and have suffered "anxiety, sleep disruption, stress, fear, and frustration" that "go far beyond allegations of mere worry or inconvenience," *id.* ¶¶ 49, 61, 72. They have suffered injury from the exposure of their PII and PHI in violation of their right to privacy, diminution in value of that information, and an increased risk of fraud, misuse, and identity theft. *Id.* ¶¶ 50-52, 62-64, 73-75. They anticipate spending money to try to mitigate future injuries. *Id.* ¶¶ 53, 65, 76.

Plaintiffs allege that stolen PII and PHI is valuable and is often traded and sold on the dark web. *Id.* ¶¶ 79-80. Criminals often combine stolen PII and PHI with unregulated data found elsewhere on the internet like phone numbers, emails, and addresses into "Fullz" packages, which are comprehensive dossiers about individuals. *Id.* ¶ 81. Plaintiffs allege that IMA's failure to notify them "promptly and properly" about the data breach deprived them of the ability to act early and take measures to protect their information and mitigate the harm of the data breach. *Id.* ¶ 96.

Plaintiffs bring a class action on behalf of all individuals whose information was compromised in the data breach. *Id.* ¶ 134. They bring claims for (1) negligence, (2) negligence per se based on violation of the Federal Trade Commission Act ("FTCA") and the Health Insurance Portability and Accountability Act ("HIPAA"), (3) negligence per se based on violation of Kansas consumer protection law, (4) breach of implied contract, (5) unjust enrichment, and (6) invasion of privacy. They seek monetary damages, as well as declaratory and injunctive relief.

IMA moves to dismiss under Rule 12(b)(1) and Rule 12(b)(6). Its arguments under Rule 12(b)(1) are based on standing. Doc. 24 at 4. It asserts both a facial and factual attack on the standing of Plaintiffs to bring the claims asserted. *Id.* at 4-5. IMA also challenges each of Plaintiffs' claims under Rule 12(b)(6) for failure to state a plausible claim. *See* Doc. 23 at 1-2.

II. STANDARD

Although IMA moves to dismiss under both Rule 12(b)(1) and Rule 12(b)(6), the Court concludes that the analysis under Rule 12(b)(1) is dispositive and thus only states that standard.

Motions to dismiss for lack of jurisdiction under Rule 12(b)(1) can generally take two forms: a facial attack or a factual attack. "[A] facial attack on the complaint's allegations as to [subject-matter] jurisdiction questions the sufficiency of the complaint." *Holt v. United States*, 46 F.3d 1000, 1002 (10th Cir. 1995), *abrogated on other grounds by Cent. Green Co. v. United States*, 531 U.S. 425, 437 (2001). In that situation, the allegations in the complaint are accepted as true. *Id.* A factual attack looks beyond the operative complaint to the facts on which subject-matter jurisdiction depends. *Id*. at 1003.

III. ANALYSIS

IMA challenges Plaintiffs' standing to bring this case.[2] Specifically, IMA moves to dismiss because Plaintiffs "do not and cannot plead they have suffered actual misuse of their data that caused a concrete injury traceable to the data-security incident." Doc. 24 at 3.

A. Article III Standing

Courts are not "free-wheeling enforcers of the Constitution and laws." *Initiative & Referendum Inst. v. Walker*, 450 F.3d 1082, 1087 (10th Cir. 2006). Article III of the Constitution

[2] "A putative class action can proceed as long as one named plaintiff has standing." *In re SuperValu, Inc.*, 870 F.3d 763, 768 (8th Cir. 2017).

specifically limits the jurisdiction of federal courts to cases and controversies. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 559 (1992). In other words, the Constitution requires that plaintiffs have standing to bring claims. *See United States v. Colo. Supreme Court*, 87 F.3d 1161, 1164 (10th Cir. 1996); *see also Brady Campaign to Prevent Gun Violence v. Brownback*, 110 F. Supp. 3d 1086, 1091 (D. Kan. 2015) ("One of several doctrines reflecting Article III's case-or-controversy limitation on the judicial power is the doctrine of standing.").

The burden of alleging standing is on the plaintiff. *Ward v. Utah*, 321 F.3d 1263, 1266 (10th Cir. 2003) A plaintiff can do this by showing "that (1) he or she has suffered an injury in fact; (2) there is a causal connection between the injury and the conduct complained of; and (3) it is likely that the injury will be redressed by a favorable decision." *Id.* (quoting *Phelps v. Hamilton*, 122 F.3d 1309, 1326 (10th Cir. 1997)). At the pleading stage, general allegations of injury suffice. *Lujan*, 504 U.S. at 561. But a court need not accept "conclusory allegations, unwarranted inferences, or legal conclusions." *Brady Campaign*, 110 F. Supp. 3d at 1092. Allegations establishing standing must still meet the requisite pleading standards.

The first element of standing—injury in fact—encompasses "an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Initiative & Referendum*, 450 F.3d at 1087 (quoting *Lujan*, 504 U.S. at 560). An injury is concrete if it actually exists. *Spokeo, Inc. v. Robins*, 587 U.S. 330, 340 (2016). An imminent injury is one that is "certainly impending," *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013), or one in which there is a "substantial risk" the harm will occur, *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). But a mere risk of future harm is not enough. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210-12 (2021).

The second element—causation or traceability—requires a plaintiff to "allege a substantial likelihood that the defendant's conduct caused [the] plaintiff's injury in fact." *Santa Fe All. for Pub. Health & Safety v. City of Santa Fe, N.M.*, 993 F.3d 802, 814 (10th Cir. 2021) (internal quotation and citation omitted). The injury must not be "the result of the independent action of some third party not before the court." *Id.* (internal quotation and citation omitted). A plaintiff cannot establish that an injury is "fairly traceable" by a "speculative chain of possibilities." *Clapper*, 568 U.S. at 414.

The third element—redressability—looks to whether the relief requested will redress the injury. *Ash Creek Mining Co. v. Lujan*, 969 F.2d 868, 875 (10th Cir. 1992). This element is not at issue in this motion. The Court therefore focuses on injury and causation.

There are eight potential grounds for standing in the complaint. Some are injuries that already occurred: (1) actual misuse of data for Masterson and Abel; (2) delayed notification; (3) time spent by Plaintiffs monitoring their accounts; (4) "anxiety, sleep disruption, stress, fear, and frustration" by all Plaintiffs; (5) loss of privacy by all Plaintiffs based on exposure of PII and PHI; and (6) the diminution in value of PII and PHI for all Plaintiffs. The remaining injuries are potential: (7) risk of future fraud, misuse, or theft; and (8) future costs of mitigation.[3]

[3] This list of potential sources of standing is drawn from the complaint. The parties have largely structured their briefing around these claimed injuries. The Court notes a separate paragraph in the complaint, in which Plaintiffs allege to have suffered or are at an increased risk of suffering the following damages: (1) "loss of the opportunity to control how their Private Information is used;" (2) "diminution in value of their Private Information;" (3) "compromise and continuing publication of their Private Information;" (3) "out-of-pocket costs from trying to prevent, detect, and recover[] from identity theft and fraud;" (4) "lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, inter alia, preventing, detecting, contesting, and recovering from identify theft and fraud;" (5) "delay in receipt of tax refund monies;" (6) "unauthorized use of their stolen Private Information;" and (7) "continued risk to their Private Information—which remains in Defendant's possession—and is thus [at] risk for future[] breaches so long as Defendant fails to take appropriate measures to protect the Private Information." Doc. 19 at ¶ 78. Several of these are repetitive or arguably encompassed by the analysis as structured by the parties. Others are not supported by any pleaded facts (i.e. (3), (4), (5) in paragraph 78) and are not specifically addressed in the briefs. Regardless, the Court takes it cue from the parties and analyzes the potential sources of standing as identified by the parties in the briefing.

B. Injuries Already Incurred

1. Misuse of Data

Masterson and Abel both allege misuse of their data. Masterson alleges that he suffered misuse of his PII and PHI when unauthorized charges appeared on his Medicare explanation of benefits. Abel argues that unauthorized charges were made on her credit or debit card. IMA lodges both a facial and factual attack on these claims of misuse.

a. Facial Attack

In its facial attack, IMA argues Plaintiffs have not plausibly alleged any misuse of their data because there are no allegations that Masterson provided his Medicare information to IMA or that Abel provided her credit or debit card information, such that any misuse of that data could be traceable to IMA.

As an initial matter, Zerbe has not alleged any misuse. Thus the complaint does not allege standing as to Zerbe for any actual misuse of PII or PHI.

The Court will assume that both instances of alleged misuse—false claims using Masterson's Medicare number and fraudulent charges on Abel's credit and debit cards—establish a concrete and actual injury for purposes of standing.[4] But to establish standing, an injury must also be traceable to a defendant. This requires a plaintiff to "allege a substantial likelihood that the

[4] IMA argues that neither Masterson nor Abel has shown an actual injury because neither pleaded that they actually paid the unauthorized charges. Doc. 24 at 6-7. The Court declines to adopt this argument. An injury for the purpose of Article III standing is not limited to financial harm. *See TransUnion*, 141 S. Ct. at 2204 ("Various intangible harms can also be concrete."); *see also Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 154 (3d Cir. 2022) ("The fact that an injury is intangible—that is, it does not represent a purely physical or monetary harm to the plaintiff—does not prevent it from nonetheless being concrete . . . ."); *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) ("The Plaintiffs do not allege that they suffered fraudulent charges on their unsolicited Chase Amazon Visa credit cards, but the Supreme Court long ago made clear that [i]n interpreting injury in fact . . . standing [is] not confined to those who [can] show economic harm." (internal quotation and citation omitted)).

defendant's conduct caused plaintiff's injury in fact." *Santa Fe All. for Pub. Health & Safety*, 993 F.3d at 814 (internal quotation and citation omitted).

On this point, the allegations in the complaint fall short. As IMA argues, there are no allegations that IMA had the information Masterson and Abel claim was misused. The only link between the data breach and the claimed misuse is that the misuse came after the data breach. This does not allege a "substantial likelihood" that the data breach caused the misuse. *See Blood v. Labette Cnty. Med. Ctr.*, 2022 WL 11745549, at *5 (D. Kan. 2022) (noting that 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 (instead of, for example, opening a new account)"); *see also 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."); *cf. Hutton*, 892 F.3d at 623 (explaining facts that linked fraudulent activity to data breach).

Based on this, IMA has demonstrated in its facial challenge that there is no standing among the Plaintiffs based on actual misuse of data.

b. Factual Attack

Alternatively, the Court finds that IMA has established that Masterson and Abel lack standing in its factual attack.[5] IMA submits declarations stating that IMA never had Masterson's Medicare number or information, nor did it have Abel's credit or debit card information. Doc. 24

[5] Again, Zerbe does not allege any misuse of his data.

at 6; *see also* Doc. 24-1; Doc. 24-2. Thus, similar to the argument above, any injury suffered based on that misuse would not be causally linked to the data breach.

The Court finds that IMA's factual attack demonstrates that the harm claimed by Masterson and Abel—actual misuse of their information—is not traceable to the data breach. As discussed above, it is unclear how the misuse of any information is traceable to the data breach if IMA never had the sensitive information—Medicare information and credit/debit card numbers—that Masterson and Abel claim was misused. *See In re Illuminate Educ. Data Sec. Incident Litig.*, 2023 WL 3158954, at *2 (C.D. Cal. 2023) (noting that "it's unclear how Vitro's allegation that someone charged her debit card on a fake website can be a result of the data breach" where there were no allegations that financial information or social security numbers were compromised); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 31 (D.D.C. 2014) ("But here's the problem: No one alleges that credit-card, debit-card, or bank-account information was on the stolen tapes."); *see also Blood*, 2022 WL 11745549, at *5.

Plaintiffs respond to IMA's factual attack with three arguments as to Masterson.[6] First, they cite *Avini Health Corp. v. BioGenus LLC*, 2023 WL 2560844 (S.D. Fla. 2023), to argue that IMA's factual attack is premature because it is just an attack on the merits of the substantive claims. In *Avini*, which was a breach-of-contract case, the defendant argued that the plaintiff lacked standing because the plaintiff had not suffered an injury because there was no breach of contract. *Id.* at *2. But IMA's factual attack does not go to the merits of the substantive claims surrounding the data breach in the way the arguments in *Avini* did. Rather, IMA just contests that the claimed injuries—Masterson's false Medicare claims and Abel's credit and debit card charges—could not

[6] Plaintiffs offer no specific response as to IMA's declaration that it never had Abel's credit and debit card information.

have been caused by the data breach. This is not a premature challenge to the substantive claims but rather a proper attack on standing.

Second, Plaintiffs argue that the factual challenge ignores the allegations in the complaint about the "Fullz" packages.[7] Plaintiffs claim that the cybercriminals responsible for the data breach at IMA used the data stolen "in combination with unregulated data found elsewhere on the internet to commit credit card and medical fraud." Doc. 25 at 5. The complaint describes this "unregulated data" as "phone numbers, emails, addresses, etc." Doc. 19 at ¶ 81. But this doesn't address the evidence submitted by IMA that it never had the information that was misused. Nor do Plaintiffs explain how the combination of PII and PHI taken in the data breach (that apparently did not include Masterson's Medicare number or Abel's credit/debit card information) combined with "unregulated data" like contact information can lead to the misuse alleged, let alone how that misuse is traceable to IMA.[8] *See SAIC*, 45 F. Supp. 3d at 31-32 (noting that the plaintiffs offered "no plausible explanation for how the thief would have acquired their banking information" if that information was not included in the lost data).

Third, Plaintiffs argue that the factual attack "fails to challenge other instances of actual misuse and injuries present in the Complaint, namely the phishing call to Plaintiff Masterson and his primary care doctor that led to the unauthorized shipment of a genetic testing kit to his home." Doc. 25 at 6. In support, Plaintiff cites to a declaration submitted by Masterson. The declaration states that he received a call after the data breach from "'Apprise Diagnostics,' a medical company somehow connected with Medicare." Doc. 25-1 at 2. The company had Masterson's information,

[7] Plaintiffs include this argument in response to IMA's factual attack even though it relies on allegations in the complaint. For the same reason this argument does not overcome IMA's factual attack, it also fails to overcome the facial attack.

[8] To the extent Plaintiffs allege this enabled the phishing call of Masterson, that argument is addressed separately.

including his social security number. *Id.* Masterson provided his doctor's contact information but subsequently reported the call to his insurers and his doctor. Masterson's declaration states that, to his knowledge, he has not been involved in any other data breach that involved his social security number or insurance information.

Masterson's declaration does not show a "substantial likelihood" that the IMA data breach caused him an injury. First, his declaration does not contradict IMA's contention that it never had Masterson's Medicare information. It only says that the notice he received after the data breach stated that his "name, Social Security number, and policy number or member ID" were "potentially affected" in the data breach. *Id.* at 1. Nor does it explain how any fraudulent charge[9] from the phishing call is traceable to IMA, especially given that Masterson concedes that he provided information to the person on the call.

In sum, Plaintiffs have not plausibly alleged that they suffered any misuse of their data or that any such misuse is traceable to IMA's alleged mishandling of their sensitive information. Thus, on its face, the complaint fails to allege standing based on misuse of data. IMA's factual challenge underscores this finding, as IMA has presented evidence that IMA never had the information that Masterson and Abel claim was misused.

2. Delayed Notification

Related to the alleged misuse of data are the parties' arguments regarding delayed notification. IMA challenges Plaintiffs' standing based on claimed injury resulting from delayed notification of the data breach. *See* Doc. 24 at 9-10. It argues that, although Plaintiffs claim IMA delayed in notifying them of the data breach, they identify no injury flowing from that delay. *Id.*

[9] The complaint states that the call to Masterson's doctor resulted "in yet another unauthorized charge." Doc. 19 at ¶ 58. But Masterson's declaration states that his doctor never responded to the request for authorization. Doc. 25-1 at 2.

Plaintiffs respond that there is injury flowing from IMA's delay in notifying Plaintiffs about the data breach, namely that Masterson was not notified of the data breach until two days after the unauthorized medical services were obtained using his Medicare number. Doc. 25 at 9. As discussed above, however, any misuse alleged by Masterton is not traceable to IMA. So Masterson would not have a related injury tied to any delay in notification traceable to IMA. Further, although Plaintiffs allege that they were not able to take preventative measures to avoid the fraudulent charges because of the delay in notification, *see* Doc. 19 at ¶¶ 35-36, there are no allegations explaining what actions they were prevented from taking due to the timing of IMA's notification. Thus, the complaint does not allege standing based on any delayed notification.

3. Time Spent Monitoring Accounts

Time spent monitoring accounts is a concrete injury "if [it is] based on a threat of future injury that is certainly impending." *Blood*, 2022 WL 11745549, at *6. As the Court discusses in Section C. below, Plaintiffs' fear of future injuries is only hypothetical. Actions taken based on a hypothetical future threat does not create a concrete injury. *See Clapper*, 568 U.S. at 416 ("In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021) ("But where 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." (internal quotation and citation omitted)); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 754 (W.D.N.Y. 2017) (finding that "mitigation efforts following a data breach do not confer standing where the alleged harm is not imminent"); *SAIC*, 45 F. Supp. 3d at 28 (stating that "measures taken to prevent a future, speculative harm" do not amount to an injury-in-fact); *see also C.C. v. Med-Data Inc.*, 2022 WL 970862, at *8 (D. Kan.

2022). Accordingly, the time Plaintiffs have spent monitoring their accounts does not establish standing.

4. Anxiety, Sleep Disruption, Stress, Fear, and Frustration

Plaintiffs allege they have suffered "anxiety, sleep disruption, stress, fear, and frustration" that "go far beyond allegations of mere worry or inconvenience" due to the data breach. Doc. 19 at ¶¶ 49, 61, 72. As an initial matter, other than the claim that their emotional injuries "go far beyond" garden variety claims of worry or inconvenience, Plaintiffs plead no facts supporting this conclusory statement. *See Garland v. Orlans, PC*, 999 F.3d 432, 439-40 (6th Cir. 2021) (noting that allegations of emotional harm are generally only actionable where they are extreme). To the extent Plaintiffs claim emotional distress because of the risk of future misuse, that claim of standing fails for the same reason as it does for time spent monitoring 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*, 568 U.S. at 416; *see also Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 994 (W.D. Okla. 2021).

As discussed above, there are no allegations of misuse tied to IMA. And as discussed below, 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. *See Garland*, 999 F.3d at 440 ("Garland's anxiety is too speculative to qualify as an injury in fact because it is merely a fear of a future harm that is not 'certainly impending'—an injury insufficient under Supreme Court precedent." (quoting *Clapper*, 568 U.S. at 410)).[10]

[10] Plaintiffs do not offer any analysis as to why or how their allegations of emotional distress have created standing. Rather, they argue only that the Supreme Court has not foreclosed standing based on emotional distress. Doc. 25 at 7-8. This does not satisfy Plaintiffs' burden to establish standing.

5. Loss of Privacy

To sustain an injury based on loss of privacy, other courts have required some allegation that personal information has been viewed or "exposed in a way that would facilitate easy, imminent access." *SAIC*, 45 F. Supp. 3d at 28-29 ("Existing case law and legislation support that common-sense intuition: If no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated."). Here, however, Plaintiffs only generally allege a loss of privacy simply because there was a data breach. There are no allegations that the PII and PHI at issue was even viewed. These allegations do not create standing. *See id.* at 29 ("[U]ntil Plaintiffs can aver that their records have been viewed (or certainly will be viewed), any harm to their privacy remains speculative."); *see also C.C.*, 2022 WL 970862, at *10 ("In sum, plaintiff's standing problem here is a familiar one: she hasn't alleged any concrete or particularized harm from her alleged loss of privacy. Her loss of privacy, in and of itself, is not a concrete harm that can provide the basis for Article III standing.").

6. Diminution in Value of PII and PHI

Diminution in the value of Plaintiffs' PII and PHI is not a concrete and particularized injury sufficient to confer standing. *See Blood*, 2022 WL 11745549, at *6. As the Court held in *Blood*, there are no allegations that Plaintiffs themselves intended to sell their PII and PHI and that it is now less valuable following the data breach. *Id.* Other courts have found likewise. *Fero*, 236 F. Supp. 3d at 755 ("Courts have rejected allegations that the diminution in value of personal information can support standing."); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1088 (E.D. Cal. 2015) (finding no standing based on diminution in value of private information where the plaintiff "has not alleged that he intended to sell his PII/PHI, that he plans to sell it in the future, that he is foreclosed from doing so because of the Data Breach, or that the data breach reduces the

value of the PII/PHI he possesses"); *SAIC*, 45 F. Supp. 3d at 30 ("As to the value of their personal and medical information, Plaintiffs do not contend that they intended to sell this information on the cyber black market in the first place, so it is uncertain how they were injured by this alleged loss.").

C. Risk of Future Injuries

All Plaintiffs assert injuries in the form of (1) risk of future fraud, misuse, theft; and (2) future costs of mitigation. Whether either of these future injuries create standing turns on whether the risk of future injury is certainly impending or substantial. *See Clapper*, 568 U.S. at 409; *Susan B. Anthony List*, 573 U.S. at 158; *Sims v. Kahrs L. Offs., P.A.*, 2023 WL 2734317, at *6 (D. Kan. 2023) ("An allegation of a mere risk of future harm—without plausible allegations that such risk is either imminent or caused a separate concrete harm—cannot be the basis for standing.").

There is split of authority on the circumstances under which a risk of future injury creates standing in data breach cases. "The Tenth Circuit has not yet addressed this issue, but multiple 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." *Blood*, 2022 WL 11745549, at *7 (citing cases); *C.C.*, 2022 WL 970862, at *4 ("Thus, where no allegations of misuse are present, circuit courts have generally declined to find standing." (internal quotation and citation omitted)); *McMorris*, 995 F.3d at 301 ("[C]ourts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused—even if plaintiffs' particular data subject to the same disclosure incident has not yet been affected."); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021) ("Generally speaking, the cases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations

of actual misuse or actual access to personal data."); *Legg*, 574 F. Supp. 3d at 990 ("[W]here no allegations of misuse are present, circuit courts have generally declined to find standing.").

As discussed above, Plaintiffs have not alleged any misuse of data stolen during the data breach that is traceable to IMA. Without any misuse to date, the Court finds that the risk of future injury and any related future costs of mitigation are too attenuated to establish standing. As the Court found in *Blood*, there are "no concrete actions on which to base a conclusion that any threatened harm is 'certainly impending'" and thus "no case or controversy before the Court." *Blood*, 2022 WL 11745549, at *8 (quoting *Clapper*, 568 U.S. at 410).

IV. CONCLUSION

Plaintiffs have not met their burden to show they have standing to bring any of their claims. Accordingly, the Court lacks subject-matter jurisdiction and must dismiss this case. *See Hill v. Vanderbilt Cap. Advisors, LLC*, 702 F.3d 1220, 1224 (10th Cir. 2012).[11] It does not reach any arguments asserted by IMA under Rule 12(b)(6).

THE COURT THEREFORE ORDERS that Defendant's motion (Doc. 23) is GRANTED. Plaintiffs' claims are dismissed without prejudice for lack of subject-matter jurisdiction.

IT IS SO ORDERED.

Dated: December 14, 2023

/s/ Holly L. Teeter
HOLLY L. TEETER
UNITED STATES DISTRICT JUDGE

[11] In their response, Plaintiffs request leave to conduct limited discovery on standing in the alternative to dismissal. Doc. 25 at 3. But they do not elaborate or explain what discovery would be needed. Nor is it clear how discovery would change the analysis on standing given that the primary deficiency is with Plaintiffs' ability to state an injury. Any injury sustained by Plaintiffs should already be known to them.