IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

C.C., individually and on behalf of all others similarly situated,

Plaintiff,

v.

MED-DATA INCORPORATED,

Defendant.

Case No. 21-2301-DDC-GEB

MEMORANDUM AND ORDER

This case is the latest entry in a growing field of data breach litigation. Data breach cases present unique Article III standing questions. Plaintiff, on behalf of herself and a proposed class, filed this action after her personal data allegedly was compromised in defendant Med-Data Incorporated's data breach. Plaintiff alleges that the data breach has caused her to sustain: (i) a loss of privacy, (ii) an "imminent, immediate and continuing risk" of identity theft and fraud, (iii) out-of-pocket expenses for her prophylactic measures and time devoted to mitigate her risk, and (iv) the lost benefit of her bargain with defendant. But plaintiff never alleges that anyone has misused her data.

Defendant filed a Motion to Dismiss (Doc. 14) under Fed. R. Civ. P. 12(b)(6) for failure to state a claim. Before the court can consider whether plaintiff's Petition states a claim, the court must determine whether plaintiff has Article III standing to bring this lawsuit. Based on the pleaded factual allegations, the court concludes that plaintiff and the proposed class do not have Article III standing. And since Article III standing is an essential ingredient for subject matter jurisdiction in federal court, the court lacks subject matter jurisdiction over this action. It

thus must remand the case to state court. The court explains this decision, below.

I. Factual Background[1]

Defendant Med-Data is a health care provider and, as part of its business, collects and maintains patient protected health information (PHI) and personally identifiable information (PII). Doc. 1 at 18 (Pet. ¶¶ 17–18). Plaintiff was a patient of defendant's "Business Associates" and provided defendant with PHI and PII.[2] *Id.* at 19 (Pet. ¶ 19).

On March 31, 2021, defendant sent plaintiff a letter informing her of a data breach. *Id.* (Pet. ¶ 23). According to defendant's notice, plaintiff's data was "uploaded to a public facing website." *Id.* (Pet. ¶ 24). And the data "was stolen, compromised, and wrongfully disseminated without authorization." *Id.* at 20 (Pet. ¶ 29). The letter reported that defendant had discovered the breach on December 10, 2020. *Id.* at 19 (Pet. ¶ 24). The data included names, social security numbers, physical addresses, dates of birth, telephone numbers, medical conditions, and diagnoses. *Id.* (Pet. ¶ 25). This breach affected tens of thousands of defendant's patients. *Id.* (Pet. ¶ 28). Plaintiff alleges that "the criminal(s) and/or their customers now have Plaintiff's and other Class Members' compromised PHI and PII." *Id.* at 24 (Pet. ¶ 51).

II. Procedural Background

Plaintiff filed this action on April 20, 2021, in the District Court of Johnson County, Kansas. *See* Doc. 1 at 15. Plaintiff asserted seven claims: outrageous conduct, breach of

---

[1] The following facts come from plaintiff's Petition, attached to defendant's Notice of Removal (Doc. 1). The court accepts these facts as true and views them in the light most favorable to plaintiff. *SEC v. Shields*, 744 F.3d 633, 640 (10th Cir. 2014) ("We accept as true all well-pleaded factual allegations in the complaint and view them in the light most favorable to the [plaintiff]." (citation and internal quotation marks omitted)). The court recounts only the facts pertinent to the current motion.

[2] As discussed in more depth below, plaintiff's Petition isn't clear about her relationship with defendant. Plaintiff alleges she is a patient of defendant. Doc. 1 at 15 (Pet. ¶ 1). Then, she alleges that she's actually a patient of defendant's "Business Associates." *Id.* at 19 (Pet. ¶ 19).

implied contract, negligence, invasion of privacy by public disclosure of private facts, breach of fiduciary duty, negligent training and supervision, and negligence per se.

On July 8, 2021, defendant removed the action to this court under the Class Action Fairness Act (CAFA). *See id.* at 3. On August 5, 2021, defendant filed a Motion to Dismiss. Doc. 14. This motion contends that plaintiff has failed to state a claim under Fed. R. Civ. P. 12(b)(6). *Id.* The motion argues that the alleged damages of each claim "are too speculative and remote[.]" Doc. 15 at 7; 10–11. Plaintiff responded on September 20, 2021. Doc. 26. Though defendant challenged plaintiff's Petition on the basis that it failed to state a claim, plaintiff also saw fit to address standing in the response brief. *See id.* at 6–10. And defendant replied on November 4, 2021. Doc. 31.

Before the court can reach defendant's Motion to Dismiss for failure to state a claim, it must address the question of standing. As explained in more detail below, if plaintiff doesn't have standing then the court doesn't have subject matter jurisdiction. And, without subject matter jurisdiction, the court cannot rule on defendant's Rule 12(b)(6) Motion to Dismiss for failure to state a claim.

III. Analysis

Federal courts carry an independent responsibility to examine subject matter jurisdiction. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94–95 (1998). The court "must dismiss the cause *at any stage* of the proceedings in which it becomes apparent that jurisdiction is lacking." *Penteco Corp. Ltd. P'ship v. Union Gas Sys., Inc.*, 929 F.2d 1519, 1521 (10th Cir. 1991) (internal quotation marks and citation omitted); *see also* 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 of the United States Constitution limits federal courts' jurisdiction to "cases" and "controversies." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013). To present a case or controversy under Article III, a plaintiff must establish that she has standing to sue. *Id.* (citations omitted). "No principle is more fundamental to the judiciary's proper role in our system of government than than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 337 (2016) (quotation cleaned up).

Article III's standing analysis requires three things: (1) an "injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical[;]" (2) "a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court[;]" and (3) that it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992) (internal quotations and citations omitted). At "the pleading stage, the plaintiff must clearly allege facts demonstrating each element" of standing. *Spokeo*, 578 U.S. at 338 (quotation cleaned up). And, at the pleading stage, general factual allegations can carry plaintiff's burden to establish the elements of Article III standing because the court must "'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)). Plaintiff and the putative class "must demonstrate standing for each claim that they press and for each form of relief that they seek[.]" *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021).

The gist of the standing inquiry is "'What's it to you?'" *Id.* at 2203 (quoting Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 Suffolk U. L. Rev. 881, 882 (1983)). With these principles in mind, the court next considers the standing inquiry in data breach cases.

A. Standing in Data Breach Cases

Data breach cases present unique standing issues. The issues usually revolve around the first element of standing: injury in fact. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). The results in data breach cases are mixed. Some plaintiffs have a hard time showing that they've suffered an injury in fact.

Some Circuits have concluded that data breach victims have sustained an injury in fact. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 691–95 (7th Cir. 2015) (concluding plaintiffs had standing standing where hackers stole customer credit card numbers and explaining "customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur" (quoting *Clapper*, 568 U.S. at 410); *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"); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628–29 (D.C. Cir. 2017) (concluding plaintiffs had standing where plaintiffs alleged data breach exposed them to heightened risk of identity theft because "unauthorized party ha[d] already accessed personally

identifying data on [defendant's] servers, and it [was] much less speculative—at the very least, it [was] plausible—to infer that this party ha[d] both the intent and the ability to use that data for ill" and focusing on the "light burden of proof the plaintiffs bear at the pleading stage"); *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 621–22 (4th Cir. 2018) (concluding plaintiffs had standing where data was "misused" and plaintiffs "allege[d] that they [had] already suffered actual harm in the form of identity theft and credit card fraud"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (concluding plaintiffs had standing where plaintiffs alleged concern about increased risk of future identity theft because plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1024–29 (9th Cir. 2018) (reaffirming *Krottner* post *Clapper*).

Other Circuits have concluded that data breach victims don't sustain an injury in fact merely because of a data breach. The plaintiffs in these cases thus lack standing. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 41–46 (3d Cir. 2011) (concluding data breach victims' "allegations of hypothetical, future injury do not establish standing under Article III"); *see also In re SuperValu, Inc.*, 870 F.3d 763, 769–70 (8th Cir. 2017) (concluding plaintiffs lacked standing when plaintiffs alleged that "illicit websites [were] selling their Card Information to counterfeiters and fraudsters, and that plaintiffs' financial institutions [were] attempting to mitigate their risk" because the allegations were "speculative" and "fail[ed] to allege any injury 'to the plaintiff[s]'" (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000))); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340–44 (11th Cir. 2021) (concluding plaintiffs' alleged harms of substantial future risk of identity theft, proactive mitigation costs, and conclusory allegations of unauthorized charges failed to confer

standing); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301, 303–05 (2d Cir. 2021) (noting "that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data" but ultimately concluding plaintiffs lacked standing because they "never alleged that their data was intentionally targeted or obtained by a third party," failed to allege their data "was in any way misused," and likewise failed to allege "that the PII was intentionally taken by an unauthorized third party or otherwise misused").

Unfortunately, our Circuit hasn't sided with either line of cases. It just hasn't had to address the question.

Some cases have tried to resolve the question by concluding that the decisions by various Circuits aren't really contradictory. For example, the Eleventh Circuit pointed out that the decisions that "conferr[ed] 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." *Tsao*, 986 F.3d at 1340. For example, in *Remijas*, 9,200 cards had sustained fraudulent charges. 794 F.3d at 690. In *Galaria*, the named plaintiff had "discovered three unauthorized attempts to open credit cards in his name." 663 F. App'x at 387. In *Krottner*, someone had tried to open a bank account in plaintiff's name after the data breach. 628 F.3d at 1142. And in *Attias*, some plaintiffs alleged they already had suffered identity theft because their tax refunds went missing. 865 F.3d at 626 n.2.

In contrast, in *In re SuperValu, Inc.*, plaintiffs alleged that their data was "stolen by hackers as a result of defendants' security practices," but the Eighth Circuit concluded that plaintiffs lacked standing because they did not allege "that [their data] was *misused*." 870 F.3d at 770 (emphasis added). Even in *Hutton*, where the Fourth Circuit found plaintiffs had standing,

the panel clarified that "a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." 892 F.3d at 621.

Thus, "where no allegations of misuse are present, circuit courts have generally declined to find standing." *Legg v. Leaders Life Ins. Co.*, ___ F. Supp. 3d ___, CIV-21-655-D, 2021 WL 5772496, at *4 (W.D. Okla. Dec. 6, 2021); *see also In re: 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1251 (M.D. Fla. 2019) ("[A]lthough the circuits have diverged in result, . . . the differing sets of facts involved in each circuit's decision are what appear to have driven the ultimate decision on standing, not necessarily a fundamental disagreement on the law."). So, the court decides, it need not wade into the deep and murky waters of a perceived Circuit split. "[I]n actuality, no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft—even those courts that have declined to find standing on the facts of a particular case." *McMorris*, 995 F.3d at 300; *see also In re: U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 58–59 (D.C. Cir. 2019) (distinguishing Third Circuit's *Reilly* because plaintiffs alleged that "cyberattackers intentionally targeted their information and point[ed] out the subsequent misuse of that information" and these were "precisely the types of allegations missing in" *Reilly*). The court thus predicts that the Tenth Circuit, if presented with the facts alleged in this case, would follow the line of cases where outcome depends on whether plaintiffs have alleged misuse of their data. Though a data breach plaintiff *may* establish standing on the basis of an increased risk of identity theft or identity fraud, plaintiff still must allege facts to show that risk "is sufficiently 'concrete, particularized, and imminent.'" *McMorris*, 995 F.3d 295, 301 (quoting *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020) (ellipsis omitted)).

In short, the court focuses its standing analysis here on the specific allegations of plaintiff's Petition. In part B, below, the court discusses two recent Supreme Court cases for additional guidance.

B. Recent Supreme Court Decisions

The Supreme Court has addressed Article III standing in two recent cases that are important to the court's standing analysis here: *Clapper* and *TransUnion*.

"Most cases declining to find standing in the data breach context rely on *Clapper*[.]" *Legg*, 2021 WL 5772496, at *5. In *Clapper*, a group of attorneys and human rights, labor, legal, and media organizations filed suit after Congress enacted the FISA Amendments Act. These amendments authorized "surveillance of individuals who are not United States persons and are reasonably believed to be located outside the United States." 568 U.S. at 401 (internal quotation marks omitted). They alleged that their work required "them to engage in sensitive international communications with individuals who they believe[d] [were] likely targets of surveillance" under 50 U.S.C. § 1881a. *Id.* These plaintiffs attempted to establish standing by asserting a future injury, *i.e.*, that there existed "an objectively reasonable likelihood that their communications will be acquired under § 1881a at some point in the future." *Id.* And, they attempted to establish a present injury—that "the risk of § 1881a-authorized surveillance already ha[d] forced them to take costly and burdensome measures to protect the confidentially of their international communications." *Id.* at 402.

The Court declined to confer standing because the plaintiffs had failed to allege an injury in fact. The Court explained: "respondents' theory of *future* injury is too speculative to satisfy the well-established requirement that the threatened injury must be certainly impending." *Id.* at 401 (citation and internal quotation marks omitted). An "objectively reasonable likelihood" of

future injury is inadequate to establish standing. *Id.* at 410. Nor could plaintiffs establish an impending injury based "on a highly attenuated chain of possibilities" and speculation. *Id.*at 410–11. And, the Court concluded, no *present* injury existed because "respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." *Id.* at 402.

In *TransUnion*, a proposed class sued TransUnion for violating the FCRA. TransUnion's files had flagged class members as "potential matches" to a federal list of serious criminals. 141 S. Ct. at 2200. The class alleged that TransUnion had failed to use reasonable procedures to ensure their credit files were accurate. *Id.* TransUnion provided some misleading credit reports about class members to third parties but, for other class members, the misleading credit reports were never sent to a third party. *Id.* The court focused its inquiry on whether plaintiffs had satisfied the "requirement that the plaintiff's injury in fact be 'concrete'—that is, 'real, and not abstract.'" *Id.* at 2204 (quoting *Spokeo*, 578 U.S. at 340).

The Court held that "the 1,853 class members whose reports were disseminated to third parties suffered a concrete injury in fact under Article III[.]" *Id.* at 2209. But the Court held that the remaining 6,332 class members whose credit reports were never sent to a third party lacked standing to sue under Article III. The Court concluded that the "mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.* at 2210.

The Court also addressed whether the 6,332 plaintiffs without a disseminated credit report adequately had asserted a risk of *future* harm. These class members argued they had "suffered a concrete injury for Article III purposes because the existence of misleading . . . alerts in their internal credit files exposed them to a material risk that the information would be

disseminated in the future to third parties and thereby cause them harm." *Id.* at 2210. The Court rejected this argument. Citing *Clapper*—and noting "importantly, *Clapper* involved a suit for *injunctive relief*"—the Court explained that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Id.* But the risk of future harm didn't suffice for these *TransUnion* plaintiffs. "[T]he 6,332 plaintiffs did not demonstrate that the risk of future harm materialized—that is," plaintiffs never alleged that TransUnion provided the misleading credit files to third parties or that the misleading files caused a denial of credit. *Id.* at 2211.

Part C, following, applies these Supreme Court precedents to the facts alleged here.

C. Whether Plaintiffs Have Alleged an Injury in Fact

Plaintiff and the putative class "must demonstrate standing for each claim that they press and for each form of relief that they seek[.]" *Id.* at 2208. The Petition at issue here asserts seven causes of action: (i) outrageous conduct, (ii) breach of implied contract, (iii) negligence, (iv) invasion of privacy by public disclosure of private facts, (v) breach of fiduciary duty of confidentiality, (vi) negligent training and supervision, and (vii) negligence per se. Doc. 1 at 32–40 (Pet. ¶¶ 79–132). Plaintiff seeks damages and injunctive relief. *Id.* (Pet. ¶ 11). And plaintiff alleges six forms of damages:

> 1. The "imminent, immediate and continuing risk of identity theft, identity fraud and/or medical fraud[;]"
>
> 2. "[O]ut-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance, and/or other Breach risk mitigation products[;]"
>
> 3. "[O]ut-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the

Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze[;]"

4. The "value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach[;]"

5. The "lost benefit of their bargain when they paid for their privacy to be protected and it was not[;]" and

6. Loss of privacy.

Doc. 1 at 29–30 (Compl. ¶ 68). None of these harms can satisfy the injury in fact requirement of Article III standing.

1. *Lupia* and HIPAA

Plaintiff's primary argument contends that the court should rely on the Health Insurance Portability and Accountability Act (HIPAA) and the Circuit's decision in *Lupia v. MediCredit, Inc.* to confer standing in this case. The Petition here discusses HIPAA at length. *See, e.g.*, Doc. 1 at 20–24 (Pet. ¶¶ 33–48). But, the problem for plaintiff is that HIPAA doesn't create a private right of action. *Wilkerson v. Shinseki*, 606 F.3d 1256, 1267 n.4 (10th Cir. 2010) (citing *Acara v. Banks*, 470 F.3d 569, 571 (5th Cir. 2006)). Instead, "HIPAA limits enforcement of the statute to the Secretary of Health and Human Services." *Acara*, 470 F.3d at 571 (citing 42 U.S.C. §§ 1320d-5, d-6). Undaunted, plaintiff argues that our Circuit "is certain" to follow its standing analysis from *Lupia v. MediCredit, Inc.*, 8 F.4th 1184 (10th Cir. 2021). Doc. 26 at 9. *Lupia*'s plaintiff demanded that defendant stop calling her about a medical debt, but the next day defendant called her anyway. 8 F.4th at 1187. Plaintiff sued under the Fair Debt Collection Practices Act (FDCPA) over this single phone call, alleging she had sustained "intangible harms, which Congress made legally cognizable in passing the FDCPA." *Id.* at 1187–88, 1190–91. The Circuit concluded that *Lupia*'s plaintiff had standing to sue.

Plaintiff concedes the principal problem with comparing this case to *Lupia*: HIPAA doesn't provide her a private right of action. In *Lupia*, the plaintiff brought two FDCPA claims under FDCPA's private right of action provision. *Id.* at 1188–89. And the *Lupia* analysis relied on Congress's recognition, when enacting the FDCPA, that certain debt collection practices cause harm. *See id.* at 1192 ("In enacting the FDCPA, Congress recognized that abusive debt-collection practices may intrude on another's privacy interests."). Thus, while the FDCPA recognized and certain harms actionable, HIPAA does no such thing. Plaintiff's *Lupia* argument doesn't persuade the court because the standing issue here isn't like the standing issue there.

2. Risk of Identity Theft and Fraud

The allegations of "imminent, immediate and continuing risk of identity theft, identity fraud and/or medical fraud" don't provide a concrete injury for this plaintiff. The court realizes that plaintiff and the putative class allege that the data breach included highly sensitive data: names, Social Security numbers, addresses, dates of birth, phone numbers, medical conditions, and medical diagnoses. Doc. 1 at 19 (Pet. ¶ 25). But plaintiff doesn't allege any misuse of any of the data. A "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Hutton*, 892 F.3d at 621; *see also In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021), *cert. denied sub nom. Huang v. Spector*, 142 S. Ct. 431 (2021) (finding plaintiffs plausibly had alleged an injury in fact because some plaintiffs had their identities stolen already and "the allegations of some Plaintiffs that they have suffered injuries resulting from actual identity theft support the sufficiency of all Plaintiffs' allegations that they face a risk of identity theft").

Without any allegations of actual fraud or identity theft, plaintiff only can resort to an argument based on risk of *future* harm. Plaintiff alleges that there "is a robust international

market for the purloined PHI and PII, specifically medical information." Doc. 1 at 24 (Pet. ¶ 52). And plaintiff alleges that "the criminals and/or their customers now have Plaintiff's and other Class Members' compromised PHI and PII." *Id.* (Pet. ¶ 51). But the Petition doesn't allege any particularized facts to corroborate this fear. *See, e.g.*, *In re: 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d. at 1255 (finding plaintiffs had "adequately pleaded that their information has been accessed and/or misused" because they alleged that data was being advertised and sold online). Plaintiff here tries to foil this factual gap in her allegations by relying on research and reports about identity theft crimes, claiming they show a risk of theft and fraud. *See, e.g.*, Doc. 1 at 26 (Pet. ¶ 57). The problem with this approach is that Supreme Court rejected it in *TransUnion*.

TransUnion explained that a risk of future harm, standing alone, can't suffice to demonstrate standing on a claim for damages. 141 S. Ct. at 2211. The reports do not show the threatened injury is "certainly impending." *Clapper*, 568 U.S. at 402. For example, plaintiff, citing a Javelin Report from 2011, alleges that "[c]onsumers who received a data breach notification had a fraud incidence rate of 19% in 2011[.]" Doc. 1 at 26 (Pet. ¶ 57). A 19% risk isn't "certainly impending" harm.[3] These generalized, inspecific, vague allegations just won't do.

Nor can plaintiff rely on the assumption that the "criminals and/or their customers" will misuse the data because "speculation about the decisions of independent actors" cannot confer

[3] Plaintiff cites other statistics, but they don't furnish any light for the alleged harms. Plaintiff alleges that, according to a 2011 Javelin Report, "consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification." Doc. 1 at 26 (Pet. ¶ 57). But plaintiff doesn't share the actual rate at which "consumers who did not receive a notification" experienced identity fraud. So, the court can't tell what "9.5 times" means in this context.

standing. *Clapper*, 568 U.S. at 414. Ultimately, the court holds, plaintiff's theory of future injury in the form of identity fraud, identity theft, or medical fraud "is too speculative to satisfy the well-established requirement that the threatened injury must be 'certainly impending.'" *Clapper*, 568 U.S. at 402.

The court also must consider the Petition's request for injunctive relief. Doc. 1 at 18 (Pet. ¶ 11). A "person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion*, 141 S. Ct. at 2210. But to show a concrete injury, the Petition must show that the specified risk of future harm is "certainly impending." *Clapper*, 568 U.S. at 409. As explained above, the risk of harm here is not sufficiently imminent or substantial to confer standing, not even for a claim seeking purely injunctive relief.[4]

3. Mitigation Costs

Third, plaintiff alleges she sustained damages in the form of time spent and expense incurred mitigating the increased risk of identity theft and fraud. But plaintiff cannot "manufacture standing merely by inflicting harm on [herself] based on [her] fears of hypothetical future harm that is not certainly impending." *Id.* at 416. As another district court in our Circuit explained, "while it may have been reasonable to take some steps to mitigate the risks associated

[4] Plaintiff alleges that she's sustained emotional distress. Doc. 1 at 32 (Pet. ¶ 83). But plaintiff doesn't reference her emotional distress damages anywhere in her argument about standing. *See generally* Doc. 26. *TransUnion* contemplates that allegations of emotional distress plus a risk of future harm may suffice to confer standing. But, as demonstrated above, plaintiff is missing half of the equation: factual allegations about the risk of future harm. 141 S. Ct. at 2211. The court declines to confer standing solely based on plaintiff's unargued emotional distress allegations. *See Clapper*, 568 U.S. at 417 (holding fear of surveillance insufficient to confer standing); *see also Reilly*, 664 F.3d at 42 (holding plaintiffs failed to allege a concrete injury, including emotional distress, because they didn't allege any misuse of their data); *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 485–86 (declining to confer standing based solely on psychological consequences).

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 (first citing *Tsao*, 986 F.3d at 1344–45 ("Tsao cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft."); then citing *In re SuperValu, Inc.*, 870 F.3d at 769 ("Because 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."); and then citing *Reilly*, 664 F.3d at 46 ("Appellants' alleged time and money expenditures to monitor their financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for Appellants' claims.")).

4. Benefit of the Bargain

Plaintiff also argues that she and the putative class members have standing because they allege harm in the form of "the lost benefit of their bargain" with defendant. Doc. 1 at 17 (Pet. ¶ 8). This theory won't square with plaintiff's factual allegations about the nature of the relationship between the parties. Indeed, those allegations are something of a moving target. First, plaintiff alleges she is a patient of defendant. *Id.* at 15 (Pet. ¶ 1). Then, she alleges that she is actually a patient of defendant's business associates, and because of this relationship she provided data to defendant. *Id.* at 19 (Pet. ¶ 19). Later yet, in plaintiff's response brief, she argues a third variant of the relationship. It claims that plaintiff "agreed to provide Defendant money in exchange for Defendant's services." Doc. 26 at 22. Even later, plaintiff argues that she is a third-party beneficiary of unspecified contracts between defendant and defendant's business associates. *Id.* at 24–25. So, plaintiff's allegations aren't exactly pellucid. And without

clear factual allegations about the relationship between the parties, the court can't discern the alleged bargain—much less its intended benefit.

As best the court can tell, plaintiff relies on a harm based on an overpayment theory. That is, plaintiff claims an implied contract existed because plaintiff received healthcare services from defendant's business associates and those business associates provided plaintiff's data to defendant. Thus, plaintiff alleges, she gave defendant money in exchange for privacy, but she didn't get the privacy intended by the implied agreement and, as a result, she sustained harm.

Several cases have rejected this theory. And the court predicts that our Circuit would join those results because plaintiff's allegations are simply too thin to confer standing. So, the court follows and applies those cases here.

Based on this overpayment theory, plaintiff alleges that some "indeterminate part" of her payment to defendant's businesses associates for healthcare services went to defendant for data security. *See In re Sci. Applications Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (explaining plaintiff's overpayment theory based on plaintiffs' claim "that some indeterminate part of" insurance premium went to insurer's data privacy vendor). "[S]uch a claim is too flimsy to support standing." *Id.* Plaintiff doesn't allege that the market value of her healthcare services (plus data security) was less than what she paid. *See id.* (rejecting overpayment theory because plaintiffs didn't allege "facts that show[ed] that the market value of their insurance coverage (plus security services) was somehow less than what they paid"); *see also Legg*, 2021 WL 5772496, at *7 (rejecting plaintiff's benefit of the bargain theory of standing in insurance company data breach action where plaintiff had not "indicated that he paid any sort of [insurance] premium in exchange for data security or that the data breach diminished the value of the insurance products he received in return").

And, even if plaintiff had lost some measure of privacy and that privacy was part of the bargain for medical services, she hasn't alleged any concrete harm from the alleged data breach. If plaintiff bargained for data security, and no third party has misused her data, then plaintiff "has received exactly what she paid for[.]" *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. CV 19-MD-2904, 2021 WL 5937742, at *11 (D.N.J. Dec. 16, 2021) (rejecting benefit of the bargain theory where plaintiffs hadn't alleged that their data was accessed, stolen, or misused).

5. Loss of Privacy

Also, plaintiff and the putative class invoke an invasion of privacy tort theory—specifically, public disclosure of private facts. Doc. 1 at 35–36 (Pet. ¶¶ 98–104). And the Petition attempts to establish standing for this claim by alleging "loss of privacy" damages. *Id.* at 29 (Pet. ¶ 68). Every data breach action—whether the court has conferred or declined to confer standing—involves a loss of privacy.

Plaintiff's alleged loss of privacy damages here arise from her invasion of privacy tort claim—specifically, the tort of "public disclosure of private information" (also known as "publicity given private life"). An action for "publicity given to private life" provides:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offense to a reasonable person, and (b) is not of legitimate concern to the public.

Restatement (Second) of Torts § 652D (Am. L. Inst. 1977); *see also Froelich v. Adair*, 516 P.2d 993, 995–96 (Kan. 1973) (adopting Restatement (Second) of Torts invasion of privacy torts); *TransUnion*, 141 S. Ct. at 2208–09 (utilizing Restatement to determine whether plaintiffs had standing). A plaintiff whose private life is given publicity "may recover for the harm resulting to his reputation from the publicity." *Id.* at § 652H cmt. a.

Here, plaintiff alleges her data was "uploaded to a public facing website[.]" Doc. 1 at 19 (Pet. ¶ 24). Even if this upload qualifies as the requisite "publicity" for a public disclosure of private facts claim, plaintiff hasn't alleged a concrete harm resulted from this publicity. She hasn't alleged *any* harm to her reputation from the alleged breach. *See In re Practicefirst Data Breach Litig.*, No. 1:21-CV-00790(JLS/MJR), 2022 WL 354544, at *8 (W.D.N.Y. Feb. 2, 2022) ("[E]ven if plaintiffs could plead facts sufficient to allege the tort of public disclosure of private information, the Court would still find a lack of subject matter jurisdiction here. Indeed, this theory of standing has been rejected in the data breach context where, like in this case, plaintiffs have failed to demonstrate any concrete or particularized injury associated with the disclosure."); *see also Duqum v. Scottrade, Inc.*, No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *8 (E.D. Mo. July 12, 2016), *aff'd sub nom. Kuhns v. Scottrade, Inc.*, 868 F.3d 711 (8th Cir. 2017) ("Plaintiffs do not allege any facts demonstrating that they suffered any damages or injury due to a loss of privacy or breach of confidentiality. These theories are not sufficiently concrete to establish injury in fact and do not support standing in this case."); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015) ("Even if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury.").

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.

IV. Conclusion

Plaintiff's claims here don't require the court to take a side in the continuing debate among data privacy outcomes because plaintiff's theories of standing are inherently speculative. Plaintiff and the proposed class haven't alleged Article III standing, so the court is without

subject matter jurisdiction to hear her case. And without subject matter jurisdiction, the court cannot address the merits of defendant's Motion to Dismiss.

The court's standing conclusion leaves one more decision: what's next? Typically, when a district court decides it lacks subject matter jurisdiction over an action, it "must dismiss the action." Fed. R. Civ. P. 12(h)(3). But 28 U.S.C. § 1447(c)—"which applies to cases" that, like this one, are "removed from state court"—provides that if it appears before final judgment "'that the district court lacks subject matter jurisdiction, the case shall be remanded.'" *Kennedy v. Nat. Balance Pet Foods, Inc.*, 361 F. App'x 785, 787 (9th Cir. 2010) (quoting 28 U.S.C. § 1447(c)). In the view of the Ninth Circuit, "[t]his provision is mandatory." *Id.* The court agrees with *Kennedy* and follows its holding here. Three reasons support this conclusion.

One, § 1447(c) applies narrowly to cases, like this one, removed from state court. Fed. R. Civ. P. 12(h)(3) is a broader provision supplied for all civil cases. When two provisions conflict, as a matter of statutory construction, the federal courts generally apply the more specific provision. *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 566 U.S. 639, 645 (2012) ("It is a commonplace of statutory construction that the specific governs the general." (quotation cleaned up)). *Two*, remand more closely fits the court's reason for its jurisdictional conclusion. Standing considerations drive the court's conclusion that it lacks subject matter jurisdiction to hear this case. Those Article III standing principles may, or may not, apply to the Kansas state court where the case originated. But as a matter of comity, the state court ought to decide that question of state law—and not a federal court. *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 726 (1966) ("Needless decisions of state law should be avoided both as a matter of comity and to promote justice between the parties, by procuring for them a surer-footed reading of applicable law."). *Last*, the remand/dismiss decision, in the end, is more form than substance.

Even if the court dismissed the case, the court would dismiss it without prejudice. *Brereton v. Bountiful City Corp.*, 434 F.3d 1213, 1216 (10th Cir. 2006) ("[T]he court, having determined that it lacks jurisdiction over the action, is *incapable* of reaching a disposition on the merits of the underlying claims."). Which means, of course, that plaintiff would have the right to file the action again in state court. The court can think of no reason—much less a good reason—why plaintiff should have to pay a second filing fee to restart a case in the forum she originally selected.

The court thus remands the case to the state court where the case was pending before removal.

IT IS THEREFORE ORDERED BY THE COURT THAT defendant's Motion to Dismiss (Doc. 14) is dismissed because the court lacks subject matter jurisdiction to decide the motion. This ruling does not affect defendant's rights, whatever they are, to present a similar motion once state court proceedings resume.

IT IS FURTHER ORDERED BY THE COURT that this case is remanded to the District Court of Johnson County, Kansas. The court directs the Clerk to take all appropriate steps to accomplish this end.

IT IS SO ORDERED.

Dated this 31st day of March, 2022, at Kansas City, Kansas.

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