F.S. v. Captify Health, Inc. et al Doc. 16

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF KANSAS**

**F.S., individually and on behalf of all others similarly situated,**

**Plaintiff,**

**v.**

**CAPTIFY HEALTH, INC. et al.,**

**Defendants.**

**Case No. 23-1142-DDC-BGS**

**MEMORANDUM AND ORDER**

Plaintiff, on behalf of himself[1] and a proposed class, filed this action after his personal data allegedly was compromised in defendant Captify Health, Inc.'s[2] data breach. Plaintiff brings seven state law tort and contract claims against defendant. After removing the case to this court under the Class Action Fairness Act (Doc. 1), defendant Captify Health, Inc. then filed a Motion to Dismiss (Doc. 6). This motion requests dismissal under Rule 12(b)(6) because, defendant argues, plaintiff has failed to state a claim in each count. Before the court can consider whether plaintiff's Petition states a claim, the court must determine whether plaintiff

[1] Plaintiff's Petition uses both male and female pronouns to refer to plaintiff. *Compare* Doc. 1-1 at 2 (Pet. ¶ 1) ("This is a class action brought by Plaintiff . . . to redress Defendants' willful and reckless violations of *his* privacy rights." (emphasis added)); *with id.* at 17 (Pet. ¶ 73) ("Plaintiff brings this . . . as a class action on behalf of *herself* and the following classes[.]" (emphasis added)). The court uses male pronouns throughout this Order because that is the convention first used by the Petition. It hopes that's the correct way to refer to plaintiff.

[2] Plaintiff initially sued multiple defendants: Advent Health Service, LLC d/b/a AdventHealth Shawnee Mission, Captify Health, Inc., Your Patient Advisor, John Does 1–50, and Jane Does 1–50. Doc. 1-1 at 1 (Pet.). Plaintiff since has voluntarily dismissed defendant "Shawnee Mission Medical Center Inc. d/b/a AdventHealth Shawnee Mission." Doc. 9. Defendant Captify filed this Motion to Dismiss (Doc. 6), so the court uses "defendant" or "defendant Captify" throughout this Order to refer only to defendant Captify Health, Inc.

Dockets.Justia.com

has Article III standing to bring this lawsuit. The court, as explained below, concludes plaintiff lacks standing and dismisses this case for lack of subject matter jurisdiction. The court thus dismisses defendant's Motion to Dismiss (Doc. 6) and remands the case to state court. The court explains its decision, below.

## I. Background[3]

Defendant Captify is a healthcare provider operating in Lenexa, Kansas. Doc. 1-1 at 6 (Pet. ¶ 21). Plaintiff is an adult residing in Kansas. *Id.* at 5 (Pet. ¶ 14). Plaintiff was one of defendant's patients. *Id.* at 2 (Pet. ¶ 1). Plaintiff entrusted his Personal Health Information (PHI) and Personally Identifiable Information (PII) to defendant. *Id.* Plaintiff brings this action to recover for defendant's unauthorized disclosure of plaintiff's PHI and PII. *Id.* (Pet. ¶ 2). Plaintiff alleges that defendant betrayed his trust by failing to safeguard and protect his PHI and PII. *Id.* (Pet. ¶ 1).

In December 2022, defendant, through its "Your Patient Advisor" service, sent plaintiff and the putative class a letter notifying them of a data security incident. *Id.* at 6 (Pet. ¶ 27). This letter read:

> After receiving reports of suspicious activity on some consumer credit cards, You[r] Patient Advisor hired forensic experts to conduct an investigation into our online customer ordering platform. After a lengthy and extensive investigation, our experts discovered that our website was compromised and some of your information may have been exposed. That investigation concluded on October 13, 2022.

[3] The following facts come from plaintiff's Petition (Doc. 1-1). The court accepts the pleaded facts as true and views them in the light most favorable to plaintiff, as the party opposing the Motion to Dismiss. *Doe v. Sch. Dist. No. 1*, 970 F.3d 1300, 1304 (10th Cir. 2020) (explaining that on a motion to dismiss the court "accept[s] as true all well-pleaded factual allegations in the complaint and view[s] them in the light most favorable to" the party opposing the motion (citation and internal quotation marks omitted)).

*Id.* (Pet. ¶ 28). The information contained in the files included patients' names, Social Security numbers, physical addresses, dates of birth, telephone numbers, medical conditions, and medical diagnoses. *Id.* at 7 (Pet. ¶ 29).

Plaintiff filed this lawsuit individually and on behalf of a class of those persons similarly situated in state court in Sedgwick County, Kansas. *Id.* at 1, 2 (Pet. ¶ 1). Plaintiff alleges defendant flagrantly disregarded his privacy and property rights by intentionally, willfully, and recklessly failing to take the necessary precautions to protect plaintiff's PHI and PII from unauthorized disclosure. *Id.* at 3 (Pet. ¶ 5). Plaintiff also alleges the following damages:

- Loss of the benefit of the bargain,
- Exposure to a heightened future risk of identity theft;
- Loss of privacy and confidentiality;
- Embarrassment, humiliation, and other emotional distress;
- Loss of enjoyment of life;
- Untimely and/or inadequate notification of the data breach;
- Improper disclosure of plaintiff's PHI and PII;
- Out-of-pocket expenses incurred to mitigate the increased risk of identity theft or fraud; and
- Time spent mitigating identify theft or fraud and the increased risk of identity theft or fraud.

Doc. 1-1 at 26 (Pet. ¶¶ 127–28).

In July 2023, defendant removed the case to this court under the Class Action Fairness Act. *See* Doc. 1. Defendant then filed a Motion to Dismiss (Doc. 6), arguing plaintiff has failed to state a claim under Fed. R. Civ. P. 12(b)(6). The motion argues that plaintiff's damages are too speculative. Doc. 6 at 10. This argument implicates plaintiff's standing to bring this lawsuit.

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 address the merits of defendant's Rule 12(b)(6) Motion to Dismiss for failure to state a claim.

## II. Legal Standard

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 question of standing is not subject to waiver[.]" *United States v. Hays*, 515 U.S. 737, 742 (1995). The court must "address the issue . . . even if the parties fail to raise the issue[.]" *Id.* And 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 he has standing to sue. *Id.* (citations omitted). "[N]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 337 (2016) (citation and internal quotation marks omitted). "[S]tanding is perhaps the most important of the jurisdictional doctrines." *Hays*, 515 U.S. at 742 (citation, brackets, and internal quotation marks omitted).

Article III's standing analysis requires three things: (1) an "injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical[;]" (2) "a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . 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 quotation marks and citations omitted). At "the pleading stage, the plaintiff must clearly allege facts demonstrating each element" of standing. *Spokeo*, 578 U.S. at 338 (citation, internal quotation marks, and ellipsis omitted). And, at the pleading stage, general factual allegations can carry plaintiff's burden to establish the elements of Article III standing because the court must "'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 889 (1990)). Plaintiff 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*, 594 U.S. 413, 431 (2021).

## III. Analysis

Data breach cases present unique Article III standing questions. 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 particular concern in data breach cases is whether plaintiffs have suffered a *concrete* injury. "No concrete harm, no standing." *TransUnion*, 594 U.S. at 442.

Data breach plaintiffs often seek to recover for the *risk* of future injury. That is, data breach plaintiffs fear something—identify theft, identity fraud, spam, etc.—might happen in the future because their data has reached the hands of cybercriminals. And some data breach plaintiffs turn this fear of future harm into a *present* injury—*i.e.*, by incurring out of pocket expenses for credit monitoring or experiencing emotional distress. Some might suggest that there's a Circuit split on the issue.

Some Circuits have concluded that data breach plaintiffs have sustained an injury in fact.[4] Other Circuits have concluded that data breach plaintiffs don't sustain an injury in fact merely because of a data breach.[5] The Tenth Circuit hasn't reached the issue, which complicates things.

---

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

[5] *See O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023) ("[W]e've held that being subjected to a data breach isn't in and of itself sufficient to establish Article III standing without a nonspeculative, increased risk of identity theft."); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301, 303–05 (2d Cir. 2021) (noting "that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data" but ultimately concluding plaintiffs lacked standing because they "never alleged that their data was intentionally targeted or obtained by a third party," failed to allege their data "was in any way misused," and likewise failed to allege "that the PII was intentionally taken by an unauthorized third party or otherwise misused"); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340–44 (11th Cir. 2021) (concluding plaintiffs'

And the court has doubts whether this perceived split really is one. As this court has noted before, misuse of the comprised data is an important inflection point that explains many of the differing results. *C.C. v. Med-Data Inc.*, No. 21-2301-DDC-GEB, 2022 WL 970862, at *4 (D. Kan. Mar. 31, 2022) ("'[W]here no allegations of misuse are present, circuit courts have generally declined to find standing.'" (quoting *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 990 (W.D. Okla. 2021))).

Misuse of plaintiff's data could cause concrete, present injury—*i.e.*, fraudulent charges, bank fees from authorized account access, etc. Misuse also shows "an increased risk of identity theft or identify fraud" in the future. *Id.*; *see also Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023) (affirming that Eleventh Circuit "typically require[s] misuse of the data cybercriminals acquire from a data breach because such misuse constitutes both a 'present' injury and a 'substantial risk' of harm in the future" (quoting *Tsao*, 986 F.3d at 1343–44)). And data breach plaintiffs have several options to show misuse. For example, in *Green-Cooper*, the Eleventh Circuit found that plaintiffs' allegations "that their credit card and personal information was exposed for theft and sale on the dark web" qualified as misuse. 73 F.4th at 889–90 (internal quotation marks omitted).

Without misuse or some other form of a present injury, data breach plaintiffs must look elsewhere to show "a material risk of future harm" to "satisfy the concrete-harm requirement," at

---

alleged harms of substantial future risk of identity theft, proactive mitigation costs, and conclusory allegations of unauthorized charges failed to confer standing); *In re SuperValu, Inc.*, 870 F.3d 763, 769–70 (8th Cir. 2017) (concluding plaintiffs lacked standing when plaintiffs alleged that "illicit websites [were] selling their Card Information to counterfeiters and fraudsters, and that plaintiffs' financial institutions [were] attempting to mitigate their risk" because the allegations were "speculative" and "fail[ed] to allege any injury 'to the plaintiff[s]'" (quoting *Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000))); *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").

least to support a request for injunctive relief.[6] *TransUnion*, 594 U.S. at 435. Other Circuits have developed a three-factor test to determine "when the risk of future misuse of PII following a data breach is imminent and substantial." *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 375 (1st Cir. 2023). Those three factors are:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain the data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

*McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021).[7] These factors aren't exclusive. *Id.*

Here, plaintiff hasn't alleged any misuse of his own data. That alone puts plaintiff on shaky standing grounds. He can't allege a present injury from misuse of his data. And, without any misuse, plaintiff's potential future injury becomes more speculative. The court thus must look elsewhere for present and future injury.

Start with present injury. Plaintiff alleges he's lost the "benefit of the bargain." Doc. 1-1 at 26 (Pet. ¶ 127). Our court already has rejected this exact theory of standing. *Med-Data*, 2022 WL 970862, at *9 (collecting cases); *see also Blood v. Labette Cnty. Med. Ctr.*, No. 5:22-cv-04036-HLT-KGG, 2022 WL 11745549, at *6 (D. Kan. Oct. 20, 2022) ("[T]he alleged overpayment for medical services . . . fails to establish standing.") (collecting cases). Beyond

---

[6] In *TransUnion*, the Court explained that risk of future harm doesn't confer standing on a plaintiff seeking to recover retroactive *damages* where actual harm never occurred. 594 U.S. at 436–37. But "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.* (emphasis added). Here, plaintiff seeks both damages and injunctive relief. *See* Doc. 1-1 at 35–36 (Pet.).

[7] The First, Second, and Third Circuits all consider these three factors. *See Webb*, 72 F.4th at 375–77; *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 283 (2d Cir. 2023) (reaffirming three *McMorris* factors, post-*TransUnion*); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153–54, 157 (3d Cir. 2022).

benefit of the bargain, plaintiff alleges other present injuries: loss of privacy and confidentiality, heightened risk of future identity theft, embarrassment, humiliation, emotional distress, loss of enjoyment of life, untimely notification of the breach out-of-pocket mitigation expenses, and time spent mitigating identity theft or fraud and the increased risk of identity theft of fraud. Doc. 1-1 at 26 (Pet. ¶¶ 127–28). Loss of privacy and confidentiality are present in every data breach case, and standing alone, they don't demonstrate a concrete injury. *Med-Data*, 2022 WL 970862, at *9–10. Plaintiff's Petition also alleges that plaintiff and the class, as data breach victims, are 9.5 times more likely to suffer identity fraud and/or identity theft. Doc. 1-1 at 3–4 (Pet. ¶ 7). Unfortunately for plaintiff, "being subjected to a data breach isn't in and of itself sufficient to establish Article III standing[.]" *O'Leary*, 60 F.4th at 244. Plaintiff's Petition further alleges that he suffered resulting from delayed notification, but it doesn't allege an actual injury resulting from delayed notification. The rest of plaintiff's injuries—risk of future identity theft, emotional injuries, and time and money spent on mitigation—"are only concrete if they are based on a threat of future injury that is certainly impending." *Blood*, 2022 WL 11745549, at *6. But plaintiff here hasn't alleged a certainly impending future injury. To demonstrate this conclusion, the court applies the three-factor test articulated above.

*First*, the court asks, "whether the plaintiffs' data has been exposed as the result of a targeted attempt[.]" *McMorris*, 995 F.3d at 303 (contrasting an "intentionally targeted data theft" with internally misplaced data). "It stands to reason that data compromised in a targeted attack is more likely to be misused." *Webb*, 72 F.4th at 375 (contrasting deliberate attack by "thieves" with an inadvertent breach). Plaintiff's Petition doesn't allege targeted attempts. Instead, the Petition defines the breach as an "unauthorized disclosure[.]" Doc. 1-1 at 2 (Pet. ¶ 2). And, according to the Petition, the data breach notice just utilizes the often unforthcoming

passive voice, providing that "our website was compromised[.]" *Id.* at 6 (Pet. ¶ 28). Allegations merely of an "unauthorized disclosure" doesn't rise to the level of an intentional, third-party data theft. This first factor thus doesn't help plaintiff.

*Second*, the court asks, "whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud[.]" *McMorris*, 995 F.3d at 303. "That at least some information stolen in the data breach has already been misused . . . makes it likely that other portions of the stolen data will be similarly misused." *Webb*, 72 F.4th at 375. As already referenced, plaintiff's Petition doesn't allege that anyone has misused his data. According to the Petition, the data breach notice mentions "suspicious activity on some customer credit cards[.]" Doc. 1-1 at 6 (Pet. ¶ 28). This might sound like data misuse, but plaintiff doesn't allege that his credit card number was disclosed. Instead, plaintiff alleges that the wrongfully disclosed PHI and PII included names, Social Security numbers, physical addresses, dates of birth, telephone numbers, medical conditions, and medical diagnoses. *Id.* at 7 (Pet. ¶ 29). The Petition never alleges any misuse of *this* information. Plaintiff thus has failed to allege any facts about data misuse—of his data or anyone else's—that could nudge plaintiff's chances of future injury into an imminent one.

*Third*, the court asks, "whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *McMorris*, 995 F.3d at 303. "Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth—especially when accompanied by victims' names—makes it more likely that those victims will be subject to future identity theft or fraud." *Id.* at 302. As just mentioned, plaintiff alleges the wrongfully disclosed data included his Social Security number, name, and date of birth. Doc. 1-1 at 7 (Pet. ¶ 29). So, this factor favors plaintiff.

In sum, that's two factors to one. Plaintiff is left only with his allegation that defendant wrongfully disclosed highly sensitive information. But without any allegations of a targeted attack or any data misuse, plaintiff falls short of alleging a "risk of harm" that "is sufficiently imminent and substantial." *TransUnion*, 594 U.S. at 435–36. And without an imminent threat of harm, neither plaintiff's emotional injuries or time and expense spent mitigating the risk of identity theft can suffice to confer standing. Plaintiffs "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.

## IV. Conclusion

The court concludes that plaintiff has failed to allege a concrete injury and, as a result, he lacks standing. This conclusion means the court is without subject matter jurisdiction. And without subject matter jurisdiction, the court can't address the merits of defendant's Motion to Dismiss (Doc. 6). The court thus dismisses the motion.

Typically, if a court lacks subject matter jurisdiction, it "must dismiss the action." Fed. R. Civ. P. 12(h)(3). But in cases removed from state court, if "at any time before final judgment it appears that the district court lacks subject matter jurisdiction, the case shall be remanded." 28 U.S.C. § 1447(c); *see also O'Leary*, 60 F.4th at 246 (concluding plaintiff failed to allege concrete injury in fact and remanding to district court with instructions to remand case to state court). 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. 6) 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 THAT** that this case is remanded to the District Court of Sedgwick County, Kansas. The court directs the Clerk to take all appropriate steps to accomplish this end.

**IT IS SO ORDERED.**

**Dated this 26th day of March, 2024, at Kansas City, Kansas.**

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