WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Angela T Travis, et al., Plaintiffs, v. Assured Imaging LLC, Defendant.	No. CV-20-00390-TUC-JCH **ORDER**

Defendant Assured Imaging, LLC ("Defendant" or "Assured") moves to dismiss Plaintiffs' Amended Class Action Complaint. (Assured Imaging, LLC's Mot. to Dismiss, Doc. 12.) The motion is fully briefed. (Pls' Resp. and Opp'n to Def.'s Mot. to Dismiss, Doc. 13; Assured Imagining, LLC's Reply Br. in Supp. of Mot. to Dismiss, Doc. 14.) For the reasons set forth below, the Court will grant Assured's motion to dismiss without prejudice.

I. BACKGROUND

a. Factual Background

This case arises from a ransomware[1] attack. (Doc. 9 at ¶ 9.) On or about May 15,

[1] Plaintiffs allege that a ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker. (First Am. Class Action Comp., Doc. 9 at 8, ¶ 34.) They allege ransomware attacks are often the final piece of a multiphase coordinated cyber-attack contending that "[o]nce cyberthieves have plundered the target's systems using [malicious software], the cybercriminals unleash their ransomware virus, locking down the target's systems for a ransom." *Id*. at ¶ 35.

2020, a cyberattack launched from an Assured employee's email inbox allowed malignant software to infect Assured's computer networks. (Doc. 9 at ¶ 36.) From May 15 to May 17, 2020, Assured was unaware that its system was compromised and the cyberthieves exfiltrated patient and other data from Assured's system. *Id*. at ¶ 37. On May 19, 2020, Defendant realized that its computer system was compromised when the nonparty actors launched a targeted ransomware attack. *Id*. at ¶ 38. The ransomware attack disrupted Assured's computer network, leaving patient data stored on its network encrypted and inaccessible for multiple days. *Id*. at ¶¶ 41, 42.

In August of 2020, Assured notified potentially affected persons and governmental agencies of the ransomware attack through a Notice of Data Incident or a Notice of Data Breach. *Id*. at ¶ 44; Docs 9-1 through 9-4. The Notice of Data Incident states in part:

> **What Happened?** On May 19, 2020, Assured learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, Assured worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.
>
> Assured conducted an extensive investigation, with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. On July 1, 2020, the investigation confirmed Assured systems were accessible by an unknown actor between May 15, 2020 and May 17, 2020, and certain, limited data was exfiltrated from our systems. The investigation was unable to determine the full extent of information that was accessed by the unknown actor. In an abundance of caution, Assured performed a comprehensive review of all information stored in our systems at the time of the incident to identify the individuals whose information may have been accessible to the unknown actor. We then worked to determine the identities and contact information for potentially impacted individuals.
>
> **What information Was Involved.** The following types of patient information were present in the electronic medical records system and therefore potentially accessed and acquired by the unknown actor during

> this incident: full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of the service performed, including any recommendations on future testing. We are unaware that any of the information was misused by the unknown actor and Assured is providing this notice in an abundance of caution.

(Doc. 9 at ¶ 44.)

Plaintiffs Angela T. Travis ("Travis"), Kerri G. Peters ("Peters"), Geraldine Pineda ("Pineda") and Rebecca Dawn Kelly-Hartnett ("Kelly-Hartnett") all received medical services from Assured. *Id*. at ¶¶ 48, 58, 63, 68. Each alleges providing Assured with personal identifying information such as their name, address, phone number, email address, medical history, demographic information, and insurance information in the course of receiving services from Assured. *See Id*. at ¶¶ 49-51 (allegations regarding Travis), ¶¶ 59-61 (allegations regarding Peters), ¶¶ 64-66 (allegations regarding Pineda), and ¶¶ 69-71 (allegations regarding Kelly-Hartnett).

Each named Plaintiff received a Notice of Data Breach similar to the above-mentioned Notice of Data Incident. *See* Doc. 9-1 at pp. 2-3 (notice sent to Travis); Doc. 9-2 at pp. 2-4 (notice sent to Peters); Doc. 9-3 at p. 2 (notice sent to Pineda); Doc. 9-4 at pp. 2-5 (notice sent to Kelly-Hartnett).The Notice of Data Breach sent to each named Plaintiff states that their personal information was "potentially accessed by the unknown actor." The words "and acquired" contained in the Notice of Data Incident are not contained in the Notice of Data Breach. *See* Doc. 9-1 at p. 2 (Travis notice); Doc. 9-2 at p. 2 (Peters notice); Doc. 9-3 at p. 2 (Pineda notice); and Doc. 9-4 at p. 2 (Kelly-Hartnett notice).

Travis is a resident of Washington state. *Id*. at ¶ 1. She alleges "see[ing] a dramatic increase in targeted spam phone calls after the ransomware attack." *Id*. ¶ 53. She alleges suffering severe emotional distress, anxiety, and stress and claims she sought medical help from a mental health counselor to deal with the anxiety and stress. *Id*. at ¶ 55. She claims to have "spent hours and hours checking her credit monitoring services" and alleges being forced to expend time "fending off" targeted phishing calls. *Id*. at ¶¶ 56, 57.

Kelly-Hartnett is also a resident of Washington state. *Id*. at ¶ 4. Like Travis, she endorses experiencing an increase in targeted spam phone calls after the ransomware

attack. (Doc. 9 at ¶ 73.) She alleges suffering severe emotional distress, anxiety, and stress and claims she was forced to increase her medication in an effort to manage her anxiety and stress. *Id*. at ¶ 75. She also alleges spending time "fending off" targeted phishing calls. *Id*. at ¶ 76.

Peters and Pineda are residents of the State of New Mexico. *Id*. at ¶¶ 2-3. Neither claim to have suffered severe emotional distress or anxiety after receiving notice of the ransomware attack. Neither Peters nor Pineda endorse receiving an increased number of spam phone calls after the ransomware attack.

Plaintiffs' First Amended Class Action Complaint alleges claims of negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, unjust enrichment, and violations of two state laws. *Id*. at pp. 37, 39, 41, 45, 48, 51, 53. Plaintiffs seek to represent a class of all persons whose personal information was compromised in the ransomware attack and two subclasses of persons (one of Washington state residents and one of New Mexico state residents) whose personal information was compromised. *Id*. at ¶ 145. Plaintiffs claim damages as a result of:

(1) "being placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft" (*Id*. at ¶ 133);

(2) "fac[ing] substantial risk of out-of-pocket fraud losses such as loans [being] opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft" (*Id*. at ¶ 134);

(3) "fac[ing] substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members" (*Id*. at ¶ 135);

(4) "may[be] also incurring out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Ransomware Attack" (*Id*. at ¶ 136);

(5) "suffer[ing] a loss of value of their Private Information when it was acquired by cyber[]thieves in the Ransomware Attack" (*Id*. at ¶ 137); and

(6) "overpa[ying] for a service that was intended to be accompanied by adequate data security but was not." (Doc. 9 at ¶ 138).

b. Procedural Background

On September 11, 2020, three plaintiffs filed suit. (Class Action Comp. Doc. 1.) On October 30, 2020, Assured filed a motion to dismiss. (Assured Imaging, LLC's Mot. to Dismiss Doc. 8.) Instead of responding to Assured's motion to dismiss, the three initial plaintiffs and one new plaintiff filed the First Amended Class Action Complaint.[2] (Doc. 9.) Thereafter, Assured filed the instant (second) motion to dismiss.

II. DEFENDANT'S MOTION

Defendant argues Plaintiffs have failed to adequately allege an injury in fact for Article III standing purposes. (Doc. 12 at pp. 9-14.) Assured contends Plaintiffs' claims are "replete with allegations about potential injuries that they or any other putative class member might have suffered." *Id*. at p. 10. It argues a claimed risk of future identity fraud resulting from the ransomware attack is insufficient to establish standing. *Id*. at pp. 11-12. It asserts Plaintiffs' claimed mitigation and emotional distress injuries are also insufficient to establish Article III standing. *Id*. at pp. 13-14. Defendant also argues Plaintiffs have failed to state a claim under Rule 12(b)(6) pleading standards. *Id*. at pp. 15-24.

III. LEGAL STANDARDS

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

A Rule 12(b)(1) jurisdictional attack can be either facial or factual. *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). "A 'facial' attack asserts that the complaint's allegations are themselves insufficient to invoke jurisdiction, while a 'factual' attack asserts that the complaint's allegations, though adequate on their face to invoke jurisdiction, are untrue." *Courthouse News Serv. v. Planet*, 750 F.3d 776, 780 n.3 (9th Cir. 2014) (citing *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1035 (9th Cir. 2004)). Assured

[2] An amended complaint supersedes a previously filed complaint. *Ferdik v. Bonzelet*, 963 F.2d 1258, 1262 (9th Cir. 1992); *Hal Roach Studios v. Richard Feiner & Co.*, 896 F.2d 1542, 1546 (9th Cir. 1990). After amendment, a court treats the previous complaint as nonexistent. *Ferdick*, 963 F.2d at 1262. Assured's initial motion to dismiss addressed the initial Class Action Complaint. (Doc. 8.) As such, Defendant's initial motion to dismiss will be denied as moot.

launches a facial attack. As such, the Court takes the allegations in the First Amended Class Action Complaint as true and construes them in the light most favorable to Plaintiffs. *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003) (citing *Zimmerman v. City of Oakland*, 255 F.3d 734, 737 (9th Cir. 2001)).

b. Article III Standing

To establish standing in federal court, a plaintiff must plead sufficient facts to show the following elements:

> First, the plaintiff must have suffered 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[.] Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. Third, it must be 'likely,' as opposed to merely 'speculative,' that the injury will be redressed by a favorable decision.

Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992) (internal quotations and citations omitted). "Where, as here, a case is at the pleading stage, the plaintiff must 'clearly … allege facts demonstrating' each element." *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547 (2016), *as revised* (May 24, 2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 518, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975)). The plaintiff bears the burden to establish that the facts alleged, if proved, would confer standing on them. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158, 134 S.Ct. 2334, 189 L.Ed.2d 246 (2014) (citing *Clapper v. Amnesty International USA*, 568 U.S. 398, 410, 133 S.Ct. 1138, 1148, 185 L.Ed.2d 264 (2013)). "That a suit may be a class action … adds nothing to the question of standing, for even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong.'" *Spokeo, Inc*., 136 S.Ct. at 1547 n.6 (quoting *Simon v. Eastern Ky. Welfare Rights Organization*, 426 U.S. 26, 40 n.20, 96 S.Ct. 1917, 48 L.Ed.2d 450 (1976) (quoting *Warth*, 422 U.S. at 502, 95 S.Ct. 2197)).

Here, Defendant argues only that Plaintiffs do not satisfy the injury in fact element of Article III standing.

IV. INJURY-IN-FACT ANALYSIS

Plaintiffs' injury in fact allegations can be separated into five categories: (1) an increased risk of identity theft as a result of the ransomware attack; (2) time and money spent on increased credit monitoring post ransomware attack; (3) a loss of value in their private information; (4) overpayment for Assured's services; and (5) emotional distress and anxiety suffered after learning of the ransomware attack. The Court discusses each category below.

a. Increased Risk of Identity Theft

Plaintiffs allege they are at risk of an imminent and impending injury arising from the risk of fraud and identity theft as a direct result of the ransomware attack. They allege facing a future substantial risk of "out-of-pocket fraud losses" such as becoming obligated on a loan in their name, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and the like. They allege facing a substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes contending "potential fraudsters" could use their personal information to target their schemes more effectively to them and putative class members. (Doc. 9 at ¶¶ 133-135.)

"In order to prove an injury-in-fact in a data breach case, a plaintiff must show the harm has already occurred, there is a 'substantial risk that the harm will occur,' or that the threatened injury is 'certainly impending.'" *Dearing v. Magellan Health Inc.*, No. 2:20-CV-00747-PHX-SPL, 2020 WL 7041059, *2 (D. Ariz. Sept. 3, 2020) (slip copy) (quoting *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023 (9th Cir. 2018) (citing *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010)). "There must be a 'credible threat of real and immediate harm stemming from the theft of [data].'" *Id.* (quoting *Krottner*, 628 F.3d at 1143). The two leading cases in this circuit on Article III injury in fact in data breach cases are *In re Zappos.com* and *Krottner*. In both cases, the United States Court of Appeals for the Ninth Circuit found the plaintiffs adequately alleged the injury in fact element of Article

III standing.

In *Krottner*, someone stole a laptop from Starbucks containing the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees. 628 F.3d at 1140. Plaintiffs alleged being placed at an increased risk of future identity theft as a result of the laptop theft. The court of appeals held the plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data" reasoning:

> [w]ere Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible. On these facts however, Plaintiffs-Appellants have sufficiently alleged an injury-in-fact for purposes of Article III standing.

628 F.3d at 1143.

In re Zappos.com, Inc., arose out of a 2012 hacking that breached the servers of online retailer Zappos.com. 888 F.3d at 1023. The hackers allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers. *Id*. The district court dismissed some of the plaintiffs' claims for lack of Article III standing. *Id*. The plaintiffs appealed contending that they had standing based on, *inter alia*, the fact that the data breach put them at risk of identity theft. *Id*. Relying upon *Krottner* the court of appeals held:

> Plaintiffs allege that the type of information accessed in the Zappos breach can be used to commit identity theft…Plaintiffs also allege that their credit card numbers were within the information taken in the breach…
>
> Indeed, the plaintiffs who alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos specifically alleged that they suffered financial losses because of the Zappos data breach (which is why the district court held they had standing). Although those plaintiffs' claims are not at issue in this appeal, their alleged harm undermines Zappos's assertion that the data stolen in the breach cannot be used for fraud or identity theft. In addition, two plaintiffs whose claims are at issue in this appeal say that the hackers took over their AOL accounts

> and sent advertisements to people in their address books. Though not a financial harm, these alleged attacks further support Plaintiffs' contention that the hacker accessed information that could be used to help commit identity theft. We thus conclude that Plaintiffs have sufficiently alleged an injury in fact under *Krottner*.

888 F.3d at 1027-28 (footnote omitted).

In its motion, Defendant sets out case law demonstrating that since *Krottner* and *In re Zappos.com* district courts have more closely examined the nature of the data breach and the type of information at issue in determining whether an injury in fact for Article III standings purposes is adequately alleged in data breach cases. *See* Doc. 12 at pp. 12-13 (citing *Dearing*, 2020 WL 7041059, at *2-3; *In re Uber Tech., Inc. Data Sec. Breach Litig*., No. CV 18-2970 PSG (GJSx), 2019 WL 6522843, *4 (C.D. Cal. Aug. 19, 2019) (slip copy); *Jackson v. Loews Hotels, Inc*., No. ED CV 18-827-DMG (JCX), 2019 WL 6721637, at *3 (C.D. Cal. Jul. 24, 2019) (slip copy); *Ables v. Brooks Bros. Grp., Inc*., No. CV 17-4309-DMG (EX), 2018 WL 8806667, at *5 (C.D. Cal. Jun. 7, 2018), *am. compl. dismissed sub nom. Brett v. Brooks Bros. Grp., Inc*., No. 17-4309-DMG (EX), 2018 WL 8806668, at *3-4 (N.D. Cal. Sept. 6, 2018); and *Antman v. Uber Tech., Inc*., No. 15-CV-01175-LB, 2018 WL 2151231, at *11 (N.D. Cal. May 10, 2018)) and Doc. 14 at p. 7 (same). *See also*, *Rahman v. Marriott International, Inc*., No. SA CV 20-00654-DOC-KES, 2021 WL 346421, at *2 (C.D. Cal. Jan. 12, 2021) ("'The sensitivity of the personal information, combined with its theft' are prerequisites to finding that plaintiffs 'adequately alleged an injury in fact.'") (citation omitted.) This Court will do the same.

i. The Ransomware Attack

The Notice of Data Breach advised each Plaintiff that their personal information was present in Assured's electronic medical records system and "therefore potentially accessed by the unknown actor[…]" *See* Doc. 9-1 at p. 2 (Travis notice); Doc. 9-2 at p. 2 (Peters notice); Doc. 9-3 at p. 2 (Pineda notice); Doc. 9-4 at p. 2 (Kelly-Hartnett notice). The notice further states, "[w]e are unaware that any of this information was misused by the unknown actor and Assured is providing this notice in an abundance of caution." *Id.* The personal information at issue here is the patient's full name, address, date of birth,

patient ID, facility, treating clinician, medical history, service performed, and assessment of service performed. *See Id*.

Relying on *Dearing v. Magellan Health, Inc.*, Defendant urges the Court to find that Plaintiffs have not sufficiently alleged injury in fact. (Doc. 12 at p. 12.) In that case, the defendant Magellan Health, Inc. discovered that one of its employees fell for a phishing scheme that allowed third party access to her email account. 2020 WL 7041059, at *1. After receiving notice of the data breach from the defendant, the plaintiff sued claiming that the data breach caused her, *inter alia*, "imminent and impending injury arising from the increased risk of fraud and identity theft." *Id*. at *1, 2.

The district court held there was no evidence the information was even stolen pointing out that the notice sent to the affected parties stated that the phisher may have seen emails in the employee's account. *Id*. at *3. The potentially viewed emails contained information such as names, social security numbers, health plan ID numbers, health plan names, healthcare providers, and drug names. *Id*. District Judge Stephen P. Logan found the plaintiff "fail[ed] to show her injury is 'certainly impending' or that there is a 'substantial risk that harm will occur[]'" concluding that "her alleged risk is entirely speculative." *Id*.

In opposition, Plaintiffs focus on the fact that Assured admits to suffering a data breach through a ransomware attack and insist they "need not suffer data misuse or identity theft before [they have] an injury for standing purposes, but the data must be actually stolen and taken in a 'manner that suggests it will be misused.'" (Doc. 13 at 4.) Plaintiffs highlight language in *Dearing* that the data must be taken in a "manner that suggests it will be misused," and insist the ransomware attack Assured suffered is such a manner. As explained below, the Court disagrees with Plaintiffs.

As mentioned above, the language of the Notice of Data Breach sent to each Plaintiff does not state that Plaintiffs' personal information was stolen. *See, e.g.*, Doc. 9-1 at p. 2 ("We determined the following types of information relating to you were present in the electronic medical records system and therefore potentially accessed…"). Based upon the Notice of Data Breach—and similar to *Dearing*— "there is no evidence the [Plaintiffs']

information was even stolen."[3] *See Dearing*, 2020 WL 7041059, at *3.

Plaintiffs also rely on *In re Zappos.com* where the court of appeals determined the plaintiffs sufficiently alleged injury in fact. But there, unlike in this case, the court found injury in fact because the plaintiffs alleged that "the hacker took over their AOL accounts and sent advertisements to people in their address book." 888 F.3d at 1027-28. Plaintiffs here have not alleged their personal information was used to take over their email accounts or identities. Plaintiffs also rely upon *Krottner*. (Doc. 13 at 5.) In that case, however, it was undisputed that the unencrypted data was stolen when the laptop was stolen. 628 F.3d at 1143. Again, the Notice of Data Breach here speaks in terms of Plaintiffs' personal information having been potentially accessed.

i. The Type of Personal Information Involved

The type of personal information at issue here is an Assured patient's full name, address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of service performed. *See, e.g.*, Doc. 9-1 at p. 2 (identifying personal information). Defendant argues that the type of personal information potentially accessed through the ransomware attack does not rise to the level that is required for this Court to find a certainly impending injury in fact for Article III standing. As explained below, the Court agrees.

Defendant relies on *In re Uber Tech., Inc Data Sec. Breach Litig*. There, a plaintiff seeking to represent a putative class sued after Uber users' personally identifiable information was breached. 2019 WL 6522843, at *1. The breach occurred when two hackers accessed a private GitHub coding site used by Uber software engineers and then

[3] The HIPPA website notice attached to the First Amended Class Action Complaint states that the personal information that was contained in the database that was breached was "potentially accessed and acquired." (Rezolut – HIPPA Website Notice, Doc. 9-6 at p. 2.) This is the notice Plaintiffs appear to quote in their First Amended Class Action Complaint. (Doc. 9 at ¶ 44.) However, Plaintiffs' notices do not include the "and acquired" phrase that is contained in the HIPPA website notice. That some putative class members may have suffered theft of their personal information does not confer an injury in fact upon the named Plaintiffs. *See Spokeo, Inc*., 136 S.Ct. at 1547 n.6 (even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong) (citations and quotations omitted).

used login credentials that they obtained to discover an archive of Uber's rider and driver information. *Id*. The compromised data included the names, email addresses, and mobile phone numbers of 50 million riders and 7 million drivers and included "some 600,000 U.S. driver's license numbers." *Id*. In determining the plaintiff failed to adequately allege injury in fact, the district court held the plaintiff "fails to explain *how* gaining access to one's basic contact information and driver's license number creates a credible threat of fraud or identity theft." *Id*. at *4 (citing *Antman v. Uber Techs., Inc.*, (*Antman I*), No. 3:15-cv-01175-LB, 2015 WL 6123054, at *10-11 (N.D. Cal. Oct. 19, 2015) (similarly concluding that an allegation that a theft of names and driver's licenses, without more, is insufficient to establish a credible threat of immediate harm)) (emphasis in original). The court determined the plaintiff's allegations of an increased risk of fraud and identity theft were insufficient to establish a credible risk of immediate harm for Article III standing purposes. *Id*. at *5.

Similarly, in *Ables v. Brooks Bros. Grp., Inc.*, also relied upon by Defendant, clothing retailer Brooks Brothers suffered the installation of malware in its point-of-sale systems affecting at least 223 of its locations. 2018 WL 8806667 at *1. As a result, an unauthorized party collected the credit and debit card account numbers, expiration dates, and verification codes, as well as full names, of Brooks Brothers customers for approximately 11-months. 2018 WL 8806667 at *1. In finding that the plaintiff failed to establish standing based on an injury in fact theory stemming from a risk of future identity theft or fraudulent activity resulting from the data breach, the district court relied on the fact that the compromised information did not include addresses or social security numbers.[4] *Id*. at *5.

The district court in *Ables* also held that the first amended complaint failed to explain how "the wrongdoers' possession of [the plaintiff's] first and last name expose[d] him" to a substantial risk of future identity theft. *Id*. Finally, the court determined that even

[4] The court also determined that "cancellation of the compromised debit and credit card accounts extinguished any concrete risk of future identity theft…[.]" *Ables*, 2018 WL 8806667, at *4.

assuming that a third party "intends to commit identity theft using [the plaintiff's] compromised PII, [he] still has not made allegations that give rise to the reasonable inference that the stolen PII is sufficient to *actually commit* identity theft." *Id*. (emphasis in *Ables*). In reaching its decision, *Ables* distinguished a number of district court cases relied upon by the plaintiff in that case. *See Id*. at *6 (distinguishing *In re Adobe Sys., Inc. Privacy Litig.*, 66 F.Supp.3d 1197, 1206 (N.D. Cal. 2014) (personal information included "names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses"); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig*., 996 F.Supp.2d 942, 954 (S.D. Cal. 2014), order corrected, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) (personal information included "names, mailing addresses, email addresses, birth dates, credit and debit card information (card numbers, expiration dates, and security codes), and login credentials"); *Doe 1 v. AOL LLC*, 719 F.Supp.2d 1102, 1105 (N.D. Cal. 2010) (personal information included "names, social security numbers, addresses, telephone numbers, credit card numbers, user names, passwords, and financial/bank account information").

Defendant also points to *Jackson v. Lowes Hotels, Inc*., wherein the court determined the plaintiff failed to sufficiently allege a certainly impending future harm reasoning:

> […] Plaintiff has once again failed to demonstrate that her name, phone number, email address (but not her email password), and mailing address are sensitive enough pieces of information to give rise to a certainly impending risk of future identity theft or fraud. Her claim that she has received mass mailing materials does not help her because receiving spam or mass mail does not constitute an injury. *See, e.g., Peters v. St. Joseph Servs. Corp*., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) (no injury despite plaintiff receiving "target[ed]" physical, electronic, and telephonic "solicitations"); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("The receipt of spam by itself, however, does not constitute a sufficient injury entitling [plaintiff] to compensable relief.").

2019 WL 6721637, at *4.

Here, the personal information potentially accessed was Plaintiffs' full name,

address, date of birth, patient ID, facility, treating clinician, medical history, service performed, and assessment of service performed. In light of the case law set forth above, the Court is unconvinced that Plaintiffs are at risk of a certainly impending identity theft or fraud injury because their full name, address, date of birth (along with the other identified information) was potentially accessed in the ransomware attack.

The Court is not persuaded by the cases relied upon by Plaintiffs. For instance, Plaintiffs rely upon *In re Adobe Sys., Inc. Privacy Litig.*, pointing out that case is similar to the instant case on the grounds that "the hackers stole the customer data." (Doc. 13 at 4.) While that was true in *In re Adobe*, as explained above, that is not the case here based on the Notice of Data Breach that each Plaintiff received. *See, e.g.*, Doc. 9-1 at p. 2 ("We determined the following types of information relating to you were present in the electronic medical records system and therefore potentially accessed…"). Furthermore, the data in *In re Adobe Sys., Inc. Privacy Litig.* included "names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses." 66 F.Supp.3d at 1206. The potentially accessed data here does not include social security numbers, debit or credit card numbers, expiration dates, attendant security codes or email addresses and passwords.

Plaintiffs also rely upon *Claridge v. RockYou, Inc.*, 785 F.Supp.2d 855, 861 (N.D. Cal. 2011). There, the defendant RockYou, Inc., a publisher and developer of online services and applications for use with social networking sites such as Facebook and MySpace, suffered a cyberattack in which a hacker accessed its database and copied the email and social networking login credentials of approximately 32 million registered RockYou users. *Id.* at 859. The district court denied the defendant's request to dismiss the complaint for lack of jurisdiction reasoning, "[n]ot only is there a paucity of controlling authority regarding the legal sufficiency of plaintiff's damages theory, but the court also takes note that the context in which plaintiff's theory arises—i.e., the unauthorized disclosure of personal information via the Internet—is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts." *Id.* Ten years have passed since *Claridge* and "the unauthorized disclosure of personal information via the Internet" can no longer be characterized as "relatively new." The Court is not persuaded by *Claridge*.

In sum, the Court finds that Plaintiffs have not sufficiently alleged that their personal information was stolen in the ransomware attack. And, even if their personal information was stolen, they have not shown that the personal information at issue is sufficiently sensitive to give rise to an imminent or certainly impending injury in fact for Article III standing purposes in data breach cases.

b. Time and Money Spent Monitoring Credit

Plaintiffs allege they "may also" incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs "directly or indirectly" related to the ransomware attack. (Doc. 9 at ¶ 136.) 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, 133 S.Ct. at 1151 (citing *Pennsylvania v. New Jersey*, 426 U.S. 660, 664, 96 S.Ct. 2333, 49 L.Ed.2d 124 (1976) (*per curiam*); *National Family Planning & Reproductive Health Assn., Inc*., 468 F.3d 826, 831 (D.C. Cir. 2006)). The focus is not upon the reasonableness of the fears but upon the imminence of the future harm and whether it is certainly impending, or the risk of harm is substantial. 568 U.S. at 416, 133 S.Ct. at 1151. Without imminent harm, mitigation expenses do not meet the injury in fact requirement of standing. 568 U.S. at 416, 133 S.Ct. at 1151. *See also*, *Rahman*, 2021 WL 346421, at *2 ("As the Supreme Court has said, 'mitigation costs … rise and fall together' with claims based on the risk of future harm." (quoting *Clapper*, 568 U.S. at 402)); *Dearing*, 2020 WL 7041059, at *3 ("…[W]hen a risk of future harm is speculative, a plaintiff cannot 'manufacture standing by choosing to make expenditures based on hypothetical harm that is not certainly impending.'" (quoting *Clapper*, 568 U.S. at 401)).

As explained above, the Court determines Plaintiffs have failed to sufficiently allege they are at an imminent risk of future harm as a result of the ransomware attack. Accordingly, Plaintiffs' claimed injury from incurring mitigation costs is insufficient as a matter of law to establish Article III standing.

c. Decreased Value in Personal Information

Plaintiffs allege "suffer[ing] a loss of value" of their personal information "when it was acquired by cyber[]thieves in the [r]ansomware [a]ttack." (Doc. 9 at ¶ 137.) They claim that medical information is "especially valuable to thieves" alleging that "the asking price for medical data" is "$50 and up." (*Id*. at ¶ 128.) Plaintiffs have not alleged any facts explaining how their personal information became less valuable as a result of the ransomware attack or that they attempted to sell their personal information and could not because of the ransomware attack.

Other courts that have examined this theory of injury have declined to find that it constitutes an injury in fact for Article III standing purposes. This Court agrees. *See, e.g., In re Zappos.com, Inc.*, 108 F.Supp.3d at 954 *rev'd on other grounds by In re Zappos.com, Inc*., 888 F.3d 1020 (9th Cir. 2018) (rejecting plaintiffs' claim that the Zappos security breach deprived them of the "substantial value" of their personal information reasoning that even assuming the plaintiffs' data has value on the black market, they did not allege any facts explaining how their personal information became less valuable as a result of the breach or that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach). *See also, Dearing*, 2020 WL 7041059, at *4 (rejecting claim that alleged diminution in value of personal information constitutes a sufficient injury in fact to confer standing).

d. Overpayment for Services

Plaintiffs allege "overpa[ying] for a service that was intended to be accompanied by adequate data security but was not." (Doc. 9 at ¶ 138.) They do not explain how the ransomware attack impacted the value of the services they received from Assured. Nor do they allege facts establishing that the price they paid for the medical services they received incorporated an amount that they understood to be allocated towards the cost of protecting their personal information.

Other courts that have examined this theory of injury have declined to find that it constitutes an injury in fact for Article III standing purposes and this Court agrees. *See,*

e.g., In re Zappos.com, Inc., 108 F.Supp.3d at 962 n.5, *rev'd on other grounds by In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018) (finding plaintiffs' theory of standing failed in part because they did not "allege facts showing how the price they paid for such goods incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data"); *Jackson v. Loews Hotels, Inc.*, 2019 WL 6721637, at *2 (finding that while the second amended complaint asserts that a portion of the price that the plaintiff paid to reserve a room went to data security, the plaintiff does not allege how the room price incorporated that amount or what gave rise to the defendant's understanding that the room reservation price included funds for data security) (quotation omitted).

e. Emotional Distress and Anxiety

Plaintiffs Travis and Kelly-Hartnett[5] contend the emotional distress, anxiety and "lack of privacy" they allegedly suffered as a result of the ransomware attack constitutes sufficient injury-in-fact to confer standing. (Doc. 13 at pp. 6-7.) They rely on *Shqeirat v. U.S. Airways Group, Inc.*, 515 F.Supp.2d 984, 998 (D. Minn. 2007). *Id.* at p. 6. The Court finds *Shqeirat* distinguishable.

As pointed out by Defendant, *Shqeirat* did not address Article III standing. Rather, that case involved individuals of Middle eastern descent who were ordered to deboard a plane and subsequently arrested. They sued alleging they were arrested in violation of their constitutional rights. 515 F.Supp.2d at 988-90. One plaintiff further alleged that his social security number, contained in a police report, was publicly posted on the internet in violation of a Minnesota state law and this event caused him to suffer fear and anxiety that he may fall victim to identity fraud. *Id.* at 991. The district court held that plaintiff's allegations were sufficient to state a claim for damages under the Minnesota state law at issue. *Id.* at 998.

This Court is not persuaded by *Shqeirat* and finds its distinguishable.

[5] Plaintiffs Peters and Pineda do not allege they suffered emotional distress or anxiety as a result of the ransomware attack.

V. CONCLUSION

The Court finds Plaintiffs lack Article III standing to sue because they have not satisfied the injury in fact requirement. As such, the Court need not consider Defendant's other arguments for dismissal based on Rule 12(b)(6) pleading standards.

The Court will grant Defendant's Motion to Dismiss without prejudice with leave to amend. Although the Court finds Plaintiffs do not have standing as currently pleaded, the Court will permit amendment.

In permitting amendment, the Court points out that time passing without harm actually occurring further undermines the claim that the threat of harm is immediate, impending, or otherwise substantial. *See In re Zappos.com*, 108 F.Supp.3d at 958 ("Indeed, putting aside the legal standard for imminence, a layperson with a commonsense notion of 'imminent' would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future.")) (citation omitted). In this same vein, Plaintiffs' allegations that "there may be a substantial lag [—] measured in years [—] between when harm occurs versus when it is discovered," that "stolen data may be held for up to a year or more before being used to commit identity theft," and that they "are at an increased risk of fraud and identity theft for many years into the future[]" tends to relegate their claim that they are at an "imminent [and] immediate" risk of future injury into the realm of speculation. (Doc. 9 at ¶¶ 125, 127, 133.) *In re Zappos.com*, 108 F.Supp.3d at 959.

…

…

…

…

…

…

…

…

For the foregoing reasons,

IT IS HEREBY ORDERED GRANTING Assured Imaging, LLC's Motion to Dismiss (Doc. 12), **DISMISSING WITHOUT PREJUDICE** the First Amended Class Action Complaint (Doc. 9), and **DENYING AS MOOT** Assured Imaging, LLC's Motion to Dismiss (Doc. 8). Plaintiffs may file a second amended complaint in accordance with the applicable Federal Rules of Civil Procedure.

Dated this 10th day of May, 2021.

Honorable John C. Hinderaker
United States District Judge