

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ALBERT PATTERSON,
Plaintiff,

v.

MEDICAL REVIEW INSTITUTE OF
AMERICA, LLC,
Defendant.

Case No. [22-cv-00413-MMC](#)

**ORDER GRANTING DEFENDANT'S
MOTION TO DISMISS OR TRANSFER;
AFFORDING PLAINTIFF LEAVE TO
AMEND; VACATING HEARING;
CONTINUING CASE MANAGEMENT
CONFERENCE**

Before the Court is defendant Medical Review Institute of America, LLC's ("MRloA") Motion, filed May 31, 2022, "to Dismiss Plaintiff's Complaint Pursuant to F.R.C.P. 12(b)(1), 12(b)(6), or Transfer the Case Pursuant to 28 U.S.C. § 1404(a)." Plaintiff Albert Patterson ("Patterson") has filed opposition, to which MRloA has replied. Having read and considered the papers filed in support of and in opposition to the motion, the Court deems the matter suitable for determination on the parties' respective written submissions, VACATES the hearing scheduled for July 8, 2022, and rules as follows.

BACKGROUND

In the Complaint, Patterson alleges MRloA is an entity that "acquired, collected[,] and stored" customers' "personal health information" ("PHI") and "personally identifiable information" ("PII") "to facilitate clinical peer review of healthcare services." (See Compl. ¶¶ 1, 5.) Patterson further alleges he received a letter from MRloA, dated January 7, 2022, "informing him that his PHI/PII and/or financial information was involved" in a data breach whereby hackers "infiltrated" MRloA's "information network" and "accessed highly sensitive" data stored thereon. (See Compl. ¶¶ 2, 20.)

Based on said allegations, Patterson asserts the following nine claims for relief:

(1) “Negligence”; (2) “Confidentiality of Medical Information Act (Cal. Civ. Code § 56, et seq.)”; (3) “Invasion of Privacy”; (4) “Breach of Confidence”; (5) “Information Practices Act of 1977 (Cal. Civ. Code § 1798, et seq.)”; (6) “Breach of Implied Contract”; (7) “Breach of the Implied Covenant of Good Faith and Fair Dealing”; (8) “Unfair Business Practices (Cal. Bus. & Prof. Code § 17200, et seq.)”; and (9) “Unjust Enrichment.”¹

DISCUSSION

By the instant motion, MRloA seeks an order dismissing the above-titled action, or, in the alternative, transferring it to the District of Utah, on the grounds that (1) Patterson lacks Article III standing, (2) Patterson has failed to allege facts sufficient to support any of his claims for relief, and (3) the District of Utah is a more convenient forum. The Court first turns to the question of standing.

A district court has subject matter jurisdiction only where the plaintiff has “[s]tanding to sue” under Article III of the Constitution. See Spokeo, Inc. v. Robins, 578 U.S. 330, 337-38 (2016). To satisfy Article III’s standing requirements, (1) “the plaintiff must have suffered an injury in fact” that is “concrete and particularized” and “actual or imminent, not conjectural or hypothetical,” (2) the injury must be “fairly traceable” to the challenged conduct of the defendant, and (3) “it must be likely . . . that the injury will be redressed by a favorable decision.” See Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992) (internal quotation, citation, and alteration omitted). “The party invoking federal jurisdiction bears the burden of establishing” the elements of standing, see id. at 561, and a plaintiff who lacks standing may not “seek relief on behalf of himself or any other member of [a] class” he purports to represent, see Warth v. Seldin, 422 U.S. 490, 502

¹ The First, Third, Fourth, Sixth, Seventh, and Ninth Claims for Relief are brought on behalf of a “Nationwide Class,” defined as “[a]ll individuals within the United States of America whose PHI/PII and/or financial information was exposed to unauthorized third parties as a result of the data breach discovered on November 9, 2021.” (See Compl. ¶ 29.) The Second, Fifth, and Eighth Claims for Relief are brought on behalf of a “California Subclass,” defined as “[a]ll individuals within the State of California whose PII/PHI was stored by Defendant and/or was exposed to unauthorized third parties as a result of the data breach discovered on November 9, 2021.” (See id.)

(1975) (internal quotation and citation omitted).

A defendant seeking dismissal for lack of standing may raise a “facial” or “factual” challenge. See Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004). “In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction,” whereas, “in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction.” See id. “Once the moving party . . . convert[s] [a] motion to dismiss into a factual motion by presenting affidavits or other evidence properly brought before the court, the party opposing the motion must furnish affidavits or other evidence necessary to satisfy its burden of establishing subject matter jurisdiction.” Savage v. Glendale Union High Sch., 343 F.3d 1036, 1039 n.2 (9th Cir. 2003).

In the instant motion, MRloA, raising both facial and factual challenges, contends Patterson lacks Article III standing for the asserted reason that he has not established a cognizable injury in fact. In that regard, MRloA identifies five theories of injury on which it understands Patterson’s complaint to be based, specifically, (1) increased risk of fraud and identity theft, (2) lost time, (3) anxiety, (4) diminution in the value of PHI and PII, and (5) loss of privacy. (See Mot. at 5:20-25 (citing Compl. ¶¶ 21-24).) In his opposition, Patterson relies only on a theory of “lost time . . . associated with [the] data breach” and makes no argument with respect to the other above-referenced theories of injury. (See Opp. at 3:23-25.) As set forth below, the Court finds Patterson has not met his burden of showing he has suffered a cognizable injury.

First, with respect to an increased risk of fraud and identity theft, although Patterson alleges the hackers “accessed highly sensitive PHI/PII and financial information” from MRloA’s network (see Compl. ¶ 2), MRloA has submitted undisputed evidence that none of the information about Patterson potentially exposed in the data breach was sufficiently sensitive to create a credible risk of future fraud or identity theft (see Leichliter Decl. ¶ 10 (stating the only information regarding Patterson that was “potentially accessed by the hackers . . . consisted of a single one-page document”

containing Patterson’s name, a date, the title “Advisory,” a reference to Patterson as the “Insured” and the “Patient,” the phrase “Review Time 60 minutes,” and that the “[t]otal amount[] to be billed [was] \$327.000”)); see also In re Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1027 (9th Cir. 2018) (holding injury in fact exists where information obtained from data breach is “sufficiently sensitive” to “g[ive] hackers the means to commit fraud or identity theft”); Greenstein v. Noblr Reciprocal Exch., Case No. 21-cv-04537-JSW, 2022 WL 472183, at *4 (N.D. Cal. Feb. 15, 2022) (finding no “credible and imminent threat of future” identity theft where data breach did not involve “social security or credit card information” or other information that could be used to “open a new account in [p]laintiffs’ names or to gain access to personal accounts likely to have more sensitive information”); Antman v. Uber Techs., Inc., Case No. 3:15-cv-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (holding no “credible risk of identity theft” exists “[w]ithout a hack of information such as social security numbers, account numbers, or credit card numbers”).

Next, with respect to lost time and anxiety associated with the breach, where, as here, there is no credible threat of future identity theft, Patterson cannot “manufacture standing by inflicting harm on [himself] based on [his] fear of hypothetical future harm that is not certainly impending.” See Clapper v. Amnesty Int’l USA, 568 U.S. 398, 416 (2013); see also Greenstein (finding no injury in fact based on “time and effort spent monitoring . . . credit reports” after data breach where “risk of identity theft and fraud” was not “real and imminent”); Antman, 2015 WL 6123054, at *11 (holding “risk of identity theft must first be real and imminent[] . . . before mitigation costs establish injury in fact”); Callahan v. Ancestry.com, Inc., Case No. 20-cv-08437-LB, 2021 WL 2433893, at *4-5 (N.D. Cal. June 15, 2021) (holding, in data breach context, “anxiety and stress” without “credible threat of future identity theft” is not cognizable injury in fact).

With respect to diminution in value, although Patterson alleges a market for PHI, PII, and financial information exists on the “dark web” (see Compl ¶ 75), he does not explain how his information is “less valuable than before the breach,” nor does he allege

he “had plans to sell” or is “prevent[ed] . . . from selling such information in the future,”
see Greenstein, 2022 WL 472183, at *5-6 (holding, “to successfully demonstrate injury in
 fact by diminution in value of PI, [p]laintiff[] must establish both the existence of a market
 for her personal information and an impairment of her ability to participate in that market”
 (internal quotation and citation omitted)).²

Lastly, with respect to loss of privacy, Patterson, as MRloA points out, has not
 “allege[d] facts to show any unauthorized individual actually viewed” or misused his
 information (see Mot. at 8:7-17); rather, MRloA has submitted undisputed evidence that
 the hackers “demanded a ransom payment . . . in exchange [for] return [of] the data” and
 that, after receiving such payment from MRloA, “returned the data they had obtained”
 (see Sullivan Decl. ¶¶ 7-9); see also In re Practicefirst Data Breach Litig., Case No. 1:21-
 CV-00790 (JLS/MJR), 2022 WL 354544, at *8 (W.D.N.Y. Feb. 2, 2022) (finding no
 cognizable injury based on loss of privacy theory where there was no allegation that the
 “data . . . copied by a hacker and held hostage for payment of a fee . . . was
 ever . . . viewed by any [unauthorized] person”); Storm v. Paytime, Inc., 90 F. Supp. 3d
 359, 368 (M.D. Penn. 2015) (finding no cognizable injury where plaintiffs did not allege
 “unidentified hacker was actually able to view, read, or otherwise understand the data it
 accessed”; noting privacy is not “violated” unless unauthorized person “has viewed” or “is
 [imminently] about to view” private information (internal quotation and citation omitted));
In re Facebook, Inc., Consumer Priv. User Profile Litig., 402 F. Supp. 3d 767, 786 (N.D.
 Cal. 2019) (noting plaintiff cannot establish standing “by simply intoning that she suffered
 an intangible privacy injury”).³

² Moreover, as MRloA points out, even if Patterson could plausibly allege he
 intended to sell his information on the dark web, there is no indication that a market exists
 for his “innocuous” information that was involved in the subject data breach. (See Mot. at
 8:2-6; see also Compl. ¶ 75 (listing, as examples of “sensitive information” sold on dark
 web, “patient[s] complete [medical] record, . . . payment card numbers,” and “[s]ocial
 [s]ecurity numbers”).)

³ To the extent Patterson contends a “risk of future harm” exists because MRloA’s
 information system “remains open to attack” (see Opp. at 4:19-24), such “theory of future
 injury” is “too speculative to satisfy the . . . requirement that threatened injury must be

Accordingly, Patterson's complaint is subject to dismissal for lack of standing. The Court will, however, afford Patterson leave to amend. See Warth, 422 U.S. at 501 (holding, where defendant successfully challenges plaintiff's standing at pleading stage, district courts ordinarily should afford plaintiff leave to amend).⁴

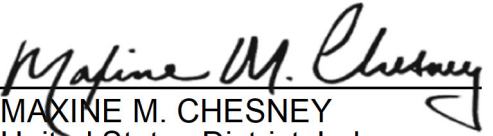
CONCLUSION

For the reasons stated above, MRloA's motion is hereby GRANTED, and the complaint is hereby DISMISSED for lack of subject matter jurisdiction. Should Patterson wish to file an amended complaint, he shall file it no later than July 14, 2022.

In light of the above, the Case Management Conference currently scheduled for August 5, 2022, is hereby CONTINUED to October 14, 2022, at 10:30 a.m. A Joint Case Management Statement shall be filed no later than October 7, 2022.

IT IS SO ORDERED.

Dated: June 23, 2022


MAXINE M. CHESNEY
United States District Judge

certainly impending," see Clapper, 568 U.S. at 401 (internal quotation, citation, and emphasis omitted).

⁴ In light of this finding, the Court does not reach MRloA's alternative arguments that Patterson has failed to state a claim and that the District of Utah is a more convenient forum.