IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 1:23-cv-01073-RM-SBP

BONNIE MASER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

COMMONSPIRIT HEALTH,

Defendant.

ORDER AND RECOMMENDATION OF UNITED STATES MAGISTRATE JUDGE

Susan Prose, United States Magistrate Judge

This matter is before this court on three motions. First, Defendant Commonspirit Health ("Defendant")'s moves (ECF No. 15) to dismiss Plaintiff Bonnie Maser's First Amended Class Action Complaint. The First Amended Complaint is filed at ECF No. 9 (stricken, clean version) and ECF No. 12-1 (redlined version) (hereafter, the "FAC"). Ms. Maser opposes the motion. ECF No. 19 ("Resp."). Defendant has replied. ECF No. 24 ("Reply"). Second, Defendant also moves (ECF No. 20) to stay discovery pending its motion to dismiss, and third, Defendant moves (ECF No. 30) for a protective order to stay the time to respond to Plaintiff's first sets of discovery requests. Plaintiff opposes those motions. ECF Nos. 28, 34. Defendant has replied. ECF Nos. 29, 37. The three motions are referred to this court under 28 U.S.C. § 636(b). ECF Nos. 16, 21, 31.

For the following reasons, this court RECOMMENDS that the motion to dismiss be

granted. This court GRANTS the motion to stay discovery and TERMINATES the motion for protective order as moot in light of granting the stay of discovery.

I. Background

Ms. Maser "brings this class action against . . . CommonSpirit . . . for its failure to properly secure and safeguard Representative Plaintiff's and Class Members' protected health information and personally identifiable information stored within Defendant's information network, including, without limitation, full names, addresses, healthcare providers, medical record numbers, treatment/prescription information, dates of medical services, other health insurance information and patient's facility/account numbers," collectively referred to as "PHI"[1] and "PII."[2] FAC ¶ 1.

She seeks "to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiff and, at least, 623,774 other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on October 2, 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and

[1] Ms. Maser defines PHI as "a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient." FAC at 2 n.1.

[2] Ms. Maser defines PII as "generally incorporat[ing] information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers etc.)." FAC at 2 n.2.

accessed highly sensitive PHI/PII, which was being kept unprotected (the "Data Breach")." *Id.* ¶ 2 (footnote omitted). She further "seeks to hold Defendant responsible for its failure to ensure that the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIP[A]A") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIP[A]A Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards." *Id.* ¶ 3.

Ms. Maser further alleges that Defendant unreasonably delayed notifying her of the Data Breach until April 5, 2023. *Id*. ¶¶ 4, 66, 91.

She alleges Defendant intentionally or negligently failed "to take and implement adequate and reasonable measures to ensure that" her (and Class Members') PHI/PII "was safeguarded," and as a result she (and Class Members) were:

> compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

Id. ¶ 9. More specifically, Ms. Maser amended her original complaint to allege that she suffered bank account fraud:

> [a]s a result of the Data Breach, cybercriminals were able to use her disclosed information to access her bank account at the local credit union. Once the criminals had access to her bank account, they drained the account and racked up over $3,000 in fraudulent charges. Later, the credit union closed the account. As Representative Plaintiff no longer had access to her funds in the account, Representative Plaintiff was unable to pay her rent and lost her housing. Additionally, as a result of the Data Breach and subsequent fraud, Representative Plaintiff's credit score dropped by over 60 points. Representative Plaintiff continues to struggle to recover from these massive losses.

Id. ¶ 21. Ms. Maser does not allege when she suffered the bank fraud.

Finally, Ms. Maser alleges that she has suffered harm in the form of panic attacks "due to the stress of the Data Breach and fraud that occurred as a result," including a panic attack "so severe that she believed that she was having a heart attack and had to been seen by emergency personnel." *Id.* ¶ 22. She claims to have "increased concerns" about her "loss of privacy" and anxiety about cybercriminals using her data. *Id.* She also alleges "lost time, annoyance, interference and inconvenience as a result of the Data Breach." *Id*.

Based on these allegations, Ms. Maser brings four claims for relief: (1) negligence; (2) breach of implied contract; (3) breach of the implied covenant of good faith and fair dealing; and (4) unjust enrichment. FAC at 21-29. She brings each claim on her own behalf and that of a nationwide class.

On August 11, 2023, Defendant filed its motion to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). ECF No. 15. Defendant argues that the court lacks subject matter jurisdiction because Ms. Maser does not allege a concrete or imminent harm to support Article III standing. Defendant also argues that Ms. Maser fails to adequately allege the minimum amount in controversy under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), and that she fails to state claims upon which relief may be granted.

Ms. Maser opposes dismissal. She argues that the theft from her credit union account — and the harms resulting from it, namely losing her housing and suffering a decrease in credit rating—are fairly traceable to the Data Breach. She further argues that she has a substantial risk of future harm (in the form of "a heightened risk of identity theft") that suffices for purposes of

standing. Resp. at 9-14.[3] Ms. Maser also argues that she has pleaded the minimum amount in controversy under CAFA, and that she states plausible claims for relief. *Id*. at 14-18. She requests an opportunity to amend if the court concludes otherwise. *Id*. at 18.

In reply, Defendant contends that Ms. Maser (1) inappropriately asserts facts in her response brief that she does not allege in the FAC; (2) relies on cases that are factually distinguishable because the data stolen in those cases was more financially-sensitive than in this case; and (3) fails to address the cases that Defendant cites on standing. Reply at 2-8. Defendant further replies that Ms. Maser fails to address the case law that shows her negligence and implied contract claims fail as a matter of law. Reply at 8-9.

II. Legal Standards

A. Rule 12(b)(1) Motions

Federal courts are courts of limited jurisdiction. Under Article III of the United States Constitution, federal courts only have jurisdiction to hear certain "cases" and "controversies," *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157 (2014), rendering them "duty bound to examine facts and law in every lawsuit before them to ensure that they possess subject matter jurisdiction." *The Wilderness Soc. v. Kane Cnty.,* 632 F.3d 1162, 1179 n.3 (10th Cir. 2011) (Gorsuch, J., concurring). Pursuant to Rule 12(b)(1), a party may bring either a facial or factual attack on subject matter jurisdiction, and a court must dismiss a complaint if it lacks subject

[3] The court refers to the page numbers of the pdf. Ms. Maser's response brief does not comply with D.C.COLO.LCivR 10.1(e), which requires double-spacing. However, as the brief appears to have only fourteen (14) pages that count under Judge Moore's practice standards, the court will assume that Ms. Maser did not exceed Judge Moore's limit of twenty pages. Counsel shall please take note, however, to comply with the court's Local Rules going forward.

matter jurisdiction. *See Pueblo of Jemez v. United States*, 790 F.3d 1143, 1147 n.4 (10th Cir. 2015). In this case, Defendant makes a facial attack. It does not rely on any factual materials outside of Ms. Maser's pleading. When the plaintiff's standing is challenged, the party invoking federal jurisdiction bears the burden of establishing it. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). *See also TransUnion LLC v. Ramirez*, 594 U.S. 413, 430-31 (2021) (same).

B. Rule 12(b)(6) Motions

"To survive a [Rule 12(b)(6)] motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Walker v. Mohiuddin*, 947 F.3d 1244, 1248-49 (10th Cir. 2020) (internal quotation marks omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). In making this determination, the "court accepts as true all well pleaded factual allegations in [the] complaint and views those allegations in the light most favorable to the plaintiff." *Straub v. BNSF Ry. Co.*, 909 F.3d 1280, 1287 (10th Cir. 2018).

Nevertheless, a plaintiff may not rely on mere labels or conclusions, "and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *see also Hall v. Bellmon*, 935 F.2d 1106, 1110 (10th Cir. 1991) (holding that litigants cannot rely on conclusory, unsubstantiated allegations to survive a Rule 12(b)(6) motion). Rather, "a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Iqbal*, 556 U.S. at 678 (internal quotation marks omitted); *see also Robbins v. Oklahoma*, 519 F.3d 1242, 1247 (10th Cir. 2008) (explaining that plausibility refers "to the scope of the allegations in a complaint," and that the allegations must

be sufficient to nudge a plaintiff's claims "across the line from conceivable to plausible").

III. Analysis

A. Defendant's Motion to Dismiss: Standing

Federal Rule of Civil Procedure 12(b)(1) permits Defendant to move to dismiss for lack of subject matter jurisdiction, including a lack of standing. A lack of standing deprives a court of subject matter jurisdiction because the judicial power of the federal courts extends only to "cases" or "controversies." U.S. Const. art. III, § 2. "The doctrine of standing," among others, "implements this" limit on our authority." *Dep't of Educ. v. Brown*, 600 U.S. 551, 561 (2023). Under that doctrine:

> [T]he irreducible constitutional minimum of standing contains three elements that a plaintiff must plead and—ultimately—prove. First, the plaintiff must have suffered an 'injury in fact' that is both *concrete and particularized and actual or imminent*, not conjectural or hypothetical. Second, the plaintiff's injury must be *fairly traceable to the challenged action* of the defendant, meaning that *there must be a causal connection* between the injury and the conduct complained of. Third, it must be 'likely,' as opposed to merely 'speculative,' that the injury will be redressed by a favorable decision.

Id. (emphasis added; cleaned up, citing *Lujan*, 504 U.S. at 560). The injury must be "real rather than abstract." *Id*. at 1190 (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)). In short, "[o]nly plaintiffs who allege a concrete injury [from the subject of their claims] have standing to sue in federal court." *Acheson Hotels, LLC v. Laufer*, 601 U.S. 1, 3 (2023).

Nonetheless, "[a]n allegation of future injury may suffice [as a concrete harm] if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted, quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). "As a general principle, 'concrete'

is not necessarily synonymous with 'tangible.' Though concreteness may be more easily satisfied for tangible injuries like physical or monetary harms, intangible injuries . . . may nevertheless be concrete for standing purposes." *Lupia v. Medicredit, Inc.*, 8 F.4th 1184, 1191 (10th Cir. 2021) (cleaned up, quoting *Spokeo*, 578 U.S. at 340); *id.* at 1193 (finding that the plaintiff sufficiently alleged a concrete harm based upon "intrusion upon seclusion" to have Article III standing to bring a claim under the Fair Debt Collection Practices Act). "In determining whether an intangible harm is sufficiently concrete to constitute an injury in fact, [the court] looks to both history and to the judgment of Congress. The [Supreme] Court has explained: history and tradition offer a meaningful guide to the types of cases that Article III empowers federal courts to consider." *Id.* at 1191 (cleaned up, citations omitted) (citing *Spokeo* and *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021), a Fair Credit Reporting Act ("FCRA") case). Specifically, the court

> consider[s] whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. Stated another way, this inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury.

Id. (cleaned up, citations omitted). "Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion*, 594 U.S. at 425.

With these general principles of standing in mind, the court turns to applying those principles to the fact-specific context that Ms. Maser alleges here: present harms from bank fraud that allegedly resulted from the Data Breach, and intangible (future) harms from an increased risk of identity theft. Thus, the main questions for evaluating Ms. Maser's standing are: (1) When

are present harms fairly traceable to a data breach, and (2) When are future risks of fraud (using the stolen or lost data) sufficiently concrete to support standing?

It appears the Tenth Circuit has not yet addressed Article III standing in a data breach case, but almost all other circuits have done so.[4] The Third Circuit, for example, helpfully summarizes the data breach cases as typically —though not exclusively—focusing on three factors:

> Courts rely on a number of factors in determining whether an injury is imminent—meaning it poses a substantial risk of harm—versus hypothetical in the data breach context. These non-exhaustive factors can serve as useful guideposts, with no single factor being dispositive to our inquiry. Among them is whether the data breach was ***intentional***. * * *
>
> Courts also consider whether the data was ***misused***. * * * Of note, misuse is not necessarily required. The Seventh Circuit has found standing despite no allegations of misuse, holding that it was sufficient that a data breach increased the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions.
>
> * * *
>
> Further, courts consider whether the ***nature of the information*** accessed through the data breach could subject a plaintiff to a risk of identity theft. For instance, disclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud. By contrast, the disclosure of financial information alone, without corresponding personal information, is insufficient. This is because financial information alone generally cannot be used to commit identity theft or fraud.

Clemens v. ExecuPharm Inc., 48 F.4th 146, 153-54 (3d Cir. 2022) (emphasis added, cleaned up, citations omitted, collecting cases). *See also* Resp. at 12 (citing e.g., *McMorris v. Carlos Lopez*

[4] This recommendation focuses on several of the circuit court data breach cases that the parties cite—and a few others that they did not—but does not attempt to exhaustively survey all of the numerous cases cited in the briefs.

& Assocs., LLC, 995 F.3d 295, 301-03 (2d Cir 2021) as focusing on the same, three non-exclusive factors for standing in data breach cases).

In other words, for purposes of analyzing Article III standing, data breach cases largely organize along three axes:

(x) intentionality of breach ("targeted" vs. "untargeted");[5]

(y) fraud-sensitivity of the exposed data; and

(z) whether there is already actual misuse of the data (fairly traceable to the data breach), or instead only a risk of future misuse (i.e., only intangible harm).

With respect to the last category, if a data breach plaintiff alleges only a risk of future misuse—intangible harm—then, consistent with *TransUnion*, *Clemens* further holds that "if the theory of injury is an unauthorized exposure of personally identifying information that results in an increased risk of identity theft or fraud, that harm is closely related to that contemplated by privacy torts that are well-ensconced in the fabric of American law." *Id.* at 155 (quotation marks omitted). But "the mere existence of a common law analog for the asserted harm does not necessarily end our inquiry. In a suit premised on the mere risk of future harm—that is, where the alleged injury-in-fact is imminent rather than actual—we must also consider the type of relief sought." *Id*. (quotation marks omitted). As to injunctive relief, a risk of future harm may suffice

[5] A "targeted" breach is one in which an unauthorized person (or persons) intentionally hacks into a defendant's network to take the personal information in its possession, or otherwise intentionally finds a way to steal the information that is in a specific defendant's possession. *See, e.g., Clemens*, 48 F.4th at 153 (collecting cases). An "untargeted" breach occurs inadvertently, when, for instance, an employee loses a laptop containing customers' or employees' unencrypted data.

if it is "sufficiently imminent and substantial." *Clemens,* 48 F.4th at 155 (quoting *TransUnion*, 141 S. Ct. at 2210; *Clapper*, 568 U.S. at 414 n.5).

But for *damages* based only on a risk of future harm, the plaintiff must allege some "additional, currently felt concrete harms" for standing. "For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services." *Id.* at 156 (citing *TransUnion*, 141 S. Ct. at 2211 n.7, analogizing to the tort of intentional infliction of emotional distress). *See also McMorris*, 995 F.3d at 303.

Of course, merely alleging emotional distress and mitigation expenses—without alleging a substantial risk of future fraud—does not in itself satisfy the concrete injury requirement:

> [W]here 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. This notion stems from the Supreme Court's guidance in *Clapper*, where it noted that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 568 U.S. at 416, 133 S. Ct. 1138.

Id. (cleaned up).

Thus, cases that involve targeted breaches, fraud-sensitive data, and actual misuse (as to at least one named plaintiff) easily meet the Article III standing requirement at the pleading phase. *See, e.g.*, *Webb v. Injured Workers Pharmacy, LLC,* 72 F.4th 365, 370 (1st Cir. 2023) (finding standing based on targeted theft of patients' data that included Social Security numbers, where a named plaintiff alleged she suffered actual tax return fraud as a result); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965 (7th Cir. 2016) (finding standing where breach was targeted, credit and debit card data was stolen, and the plaintiffs alleged actual misuse of

their credit or debit accounts after the breach); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (finding standing based on hackers' theft of customers' credit card numbers and actual fraudulent use of many of those accounts). At the opposite end, standing is easily found to be lacking in cases that involve untargeted breaches (or at least lack clarity on that issue), data that is not in itself financially-sensitive, and no actual misuse. *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 267-68 (4th Cir. 2017).

Cases that fall between those two poles come to varying conclusions depending on the alleged facts. While Ms. Maser asserts that "[g]enerally, when a claim satisfies two of these three factors, courts find standing," Resp. at 12, it is more accurate to say that if a data breach plaintiff satisfies the *intentionality* and *financial-sensitivity* factors, courts will generally find standing even when the only alleged harms are a future risk and present anxiety or mitigation expense. In this court's review, where a plaintiff asserts only a risk of future fraud, courts find standing only if the breach was targeted, the stolen data was financially-sensitive, and the plaintiff alleges at least some present emotional distress or mitigation expense. *See, e.g.*, *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 614 (9th Cir. 2021) (a case Ms. Maser cites, reflecting that the district court found standing where plaintiff alleged a targeted data breach, future risk of fraud, and mitigation time and expense, and affirming dismissal for failure to adequately allege damages to state a claim);[6] *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) (finding standing in a targeted data breach case, in which the plaintiffs whose claims were at issue in the

[6] The district court opinion makes plain, however, that the stolen data included names, birthdates, driver's license numbers, and Social Security numbers. *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1229 (D. Nev. 2020), *aff'd,* 845 F. App'x 613 (9th Cir. 2021).

appeal alleged only a risk of future harm, but the stolen data included their *credit card numbers*); *Krottner v. Starbucks Corp*., 628 F.3d 1139, 1140-43 (9th Cir. 2010) (finding standing where a laptop was stolen from the defendant, containing unencrypted names, addresses and *Social Security numbers*; allegations of an increased risk of future fraud combined with present anxiety and mitigation expenses sufficed). *See also Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 285-86 (2d Cir. 2023) (finding standing based on targeted theft of plaintiff's name and *Social Security number*, and the risk of future fraud combined with presently-felt mitigation expenses). In other words, the three factors are not as interchangeable as Ms. Maser suggests; she does not cite—nor is this court aware of—a data breach case finding standing based solely on an alleged present harm, where the plaintiff did not also allege either the stolen data was financially sensitive or that the breach was targeted.

Turning to the factual allegations here, there is no dispute that the Data Breach was *targeted*.

As for the fraud-sensitivity of the stolen data, Defendant argues that none of the stolen data fields in and of themselves can enable fraud, and in her response, Ms. Maser does not dispute this.

And as to Ms. Maser's allegations of *actual misuse versus increased risk* of future fraud, she does not allege any harm that is fairly traceable to the Data Breach. Although she alleges that her credit union account was drained as a result of the Data Breach (and as a result, she lost her housing and her credit rating was damaged), she does not allege when the bank fraud occurred in relation to the Data Breach. Nor does she allege how the PHI and specific PII that was stolen from Defendant could have enabled someone to access her financial account without

authorization. While it is tragic that Ms. Maser ultimately lost her housing and suffered a lower credit rating due to that fraud, she does not allege any facts plausibly supporting the conclusion that the theft from her account or the damage to her credit rating were fairly traceable to the Data Breach.

As for the risk of future fraud, Ms. Maser argues that the stolen data can be used for "social engineering" attacks for her more fraud-sensitive personal information, i.e., a fraudster could use the stolen data to pretend to be someone they are not, to deceive Ms. Maser or a third party into disclosing her social security or driver's license numbers, for instance. Resp. at 11. The court infers that Ms. Maser is arguing a fraudster could for instance attempt to use the disclosed relationship between herself and a specific healthcare provider or pharmacy to deceive her (or the third party) to disclose her financially-sensitive information, which they would then use to engage in fraud. Defendant replies that Ms. Maser cannot amend the FAC by way of her response brief, which is correct. *See Abdulina v. Eberl's Temp. Servs., Inc.*, 79 F. Supp. 3d 1201, 1206 (D. Colo. 2015) ("Plaintiff, however, cannot amend her complaint by adding factual allegations in response to Defendant's motion to dismiss."). But Ms. Maser also requests to be permitted leave to amend. Resp. at 18.

However, Ms. Maser does not cite any cases finding an increased risk of social engineering attacks—which *if successful* would enable future fraud—alone is an injury fairly traceable to a data breach.[7] Rather, this theory introduces an independent event into the causal

[7] There does not appear to be any uncertainty that the risk of future fraud has analogues in injuries recognized in the common law. *See, e.g.*, *Bohnak v. Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 285 (2d Cir. 2023) (citing "a well-established common-law analog: public disclosure of private facts," *Restatement (Second) Torts* § 652D (Am. L. Inst. 1977)). However, this court is

chain —someone must actually be deceived by the social engineering attack and disclose financially-sensitive information. This causal chain is too attenuated to consider the risk substantial at this point. The court therefore concludes that even if Ms. Maser had alleged the increased risk of social engineering attacks, this would not change the fact that the data stolen in the Data Breach was not financially sensitive.

Ms. Maser argues that the "intent of misusing and/or financially profiting from the information" stolen in the Data Breach "can be presumed (and it is alleged)" because "cybercriminals don't work for free." Resp. at 7 (citing FAC ¶ 9, alleging that the hacker was "an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future"). However, the intentionality of the data breach is only one of the three factors that courts consider in analyzing standing. *Cf. Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1240, 1243 (D. Colo. 2018) (in a targeted breach case, holding "a risk of future identity theft is sufficient for standing only if the data breach exposed the types of PII that can enable identity theft").

For the same reason, Ms. Maser's emotional distress and mitigation expenses and efforts are also not fairly traceable to the Data Breach.[8] As noted, without pleading a substantial risk of future fraud, these harms do not suffice for standing. *McMorris*, 995 F.3d at 303. Because Ms.

---

not aware of any common law injury analogous to a risk of future attempts to deceive.

[8] Ms. Maser also argues that she has suffered embarrassment from the Data Breach, citing FAC ¶ 37, but the cited paragraph is not on point. Rather, the FAC refers to embarrassment only in the negligence claim, where Ms. Maser alleges that she and the Class Members have been injured in having to "research[] how to prevent, detect, contest, and recover from embarrassment and identity theft." *Id.* ¶ 115. This allegation does not suggest that Ms. Maser has actually yet suffered an embarrassment from the disclosure of her PHI and PII.

Maser has not alleged a substantial risk of future harm from the Data Breach, it is irrelevant that Colorado law and the *Restatement (Second) of Torts* § 919(1) (Am. Law. Inst. 1975), generally recognize out-of-pocket and mitigation expenses as damages.

Moreover, although Ms. Maser's class-wide allegations assert that she (and the Class Members) face an increased risk of "medical identity theft" from the theft of their PHI, her response brief mentions this type of future harm only once and without any explanation. Resp. at 10 (citing FAC ¶ 37). The paragraph of her complaint that Ms. Maser cites also does not actually allege medical identity theft. Rather, those allegations appear only in her class-wide allegations. FAC ¶¶ 84-87. Ms. Maser asserts that medical identity theft occurs when an unauthorized person uses stolen medical information to pretend to be their victim, in order to obtain healthcare for themselves. She further alleges that "a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all." *Id*. ¶ 87. However, Ms. Maser does not allege that she has experienced medical identity theft herself; she does not allege any fraudulent use of her healthcare insurance or of her medical information. The class allegations of a heightened risk of this type of future fraud do not support standing for Ms. Maser.

Ms. Maser also alleges that her PHI and PII are less valuable after the Data Breach (FAC ¶ 24), citing *In re Facebook Privacy Litig*., 572 F. App'x 494, 494 (9th Cir. 2014), and a district court opinion following it, *Svenson v. Google Inc*., No. 13-cv-04080-BLF, 2015 WL 1503429, at *5 (N.D. Cal. Apr. 1, 2015). In a terse opinion, the Ninth Circuit deemed the plaintiffs' allegation

that they "los[t] the sales value of that [personal] information" which Facebook disclosed to third parties, as satisfying the damages element for their contract and fraud claims under California law. *Id*. The opinion does not analyze whether the plaintiffs in that case alleged they could and would have "sold" their personal information at a higher value if Facebook had not already disclosed it. *Svenson* followed *Facebook Privacy* in not requiring detailed allegations of such a "personal information" market, but more recent cases reflect that "the Ninth Circuit's conclusion, with respect to the contract claim, is undermined by more recent California authority." *C.M. v. MarinHealth Med. Grp., Inc.*, No. 23-CV-04179-WHO, 2024 WL 217841, at *2 n.5 (N.D. Cal. Jan. 19, 2024) (citing *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (2022), *review denied* (Dec. 14, 2022) (rejecting "lost-value-of-PII theory" to support standing for UCL *and* breach of contract claim, where plaintiffs failed to plead they "attempted or intended to participate in [the PII] market, or otherwise to derive economic value from their PII. Nor did they allege that any prospective purchaser of their PII might learn that their PII had been stolen in this data breach and, as a result, refuse to enter into a transaction with them, or insist on less favorable terms."). Here, Ms. Maser, does not allege that she could or would have sold her PHI or PII if Defendant had not been hacked. Rather, she wished for that information to remain private.

Ms. Maser also argues that her "loss of privacy" in itself supports standing. Resp. at 13-14 (citing FAC ¶ 24). *See also, e.g.,* FAC ¶ 22 (alleging concern over loss of privacy), ¶¶ 3, 58-61 (alleging a "HIPAA Privacy Rule" and other regulations applied to the data at issue), ¶ 116 (alleging in connection with negligence claim "loss of privacy" as one of Plaintiff's injuries). She cites *Doe v. Chao*, 540 U.S. 614, 618, 624-25 (2004), which she characterizes as finding that

a plaintiff had standing where he was "greatly concerned and worried" by disclosure of his Social Security number and its potential consequences. But in *Doe*, the plaintiff in question argued he was entitled to statutory minimum damages under the Privacy Act of 1974—a law which applies only to federal agencies—despite not alleging any actual damages from unauthorized disclosure of his Social Security number. The Court rejected that argument and held that allegations of actual damages are required for the claim, despite the statute providing a minimum of $1,000 per violation. *Id*. at 616. Here, there is no statutory claim, no statutory minimum, and (for the reasons stated above) Ms. Maser does not allege any actual injury. *Doe* accordingly offers no support for Ms. Maser's claims.

Ms. Maser also cites *In re Horizon Healthcare Servs. Inc. Data Breach Litig*., 846 F.3d 625, 638 (3d Cir. 2017) as finding that "'unauthorized disclosures of information' have long been seen as injurious." Resp. at 14; *see also id*. at 10 (citing *Spokeo*). To the extent Ms. Maser is arguing that the unauthorized disclosure of her PHI and PII is itself enough to constitute an injury in fact, that would only be correct if she brought a claim under the FCRA, the statute at issue in *Spokeo* and *Horizon Healthcare*. *Id*. at 631, 638. The FCRA created a statutory right of privacy, including a private right of action. *Id*. at 631 (citing 15 U.S.C. § 1681a(f)). *Horizon Healthcare* held (despite *Spokeo* requiring allegations of actual harm for standing, even for statutory damages) that by creating this statutory right

> Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some other future harm.

Id. at 639. In this case, Ms. Maser does not bring an FCRA claim or any other statutory claim in

which Congress may have established a lower threshold for standing.

In short, this court concludes that Ms. Maser does not allege an injury-in-fact—either present or future—that is substantial enough to support Article III standing. This court therefore respectfully RECOMMENDS granting Defendant's motion to dismiss the FAC for lack of standing. Because the court lacks subject matter jurisdiction, the court does not reach Defendant's other arguments for dismissal.

B. Motion to Stay Discovery

The court next addresses Defendant's motion to stay discovery until its motion to dismiss is resolved. Although this court is now issuing its recommendation to dismiss, the motion to stay is not moot. Judge Moore will still need to rule on the recommendation after the parties' have the opportunity to object under Rule 72.

While the Federal Rules of Civil Procedure do not expressly provide for a stay of proceedings while a motion to dismiss is pending, Rule 26(c) does permit the court, upon a showing of good cause, "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c). Further, "[t]he power to stay proceedings is incidental to the power inherent in every court to control the disposition of the causes on its docket with economy of time and effort for itself, for counsel, and for litigants. How this can best be done calls for the exercise of judgment, which must weigh competing interests and maintain an even balance." *Landis v. N. Am. Co.*, 299 U.S. 248, 254-55 (1936) (citing *Kan. City S. Ry. Co. v. United States*, 282 U.S. 760, 763 (1931)).

While staying discovery pending a ruling on a motion to dismiss is generally disfavored in this District, *see, e.g.*, *Chavez v. Young Am. Ins. Co.*, No. 06-cv-02419-PSF-BNB, 2007 WL

683973, at *2 (D. Colo. Mar. 2, 2007), this is not a hard and fast rule. "[G]ood cause may exist to stay discovery if a dispositive motion has been filed that could resolve the case and a stay does not unduly prejudice the opposing party." *Namoko v. Milgard Mfg., Inc.*, No. 06-cv-02031-WDM-MEH, 2007 WL 1063564, at *1 (D. Colo. Apr. 6, 2007). And certain questions—including whether the court has jurisdiction—should be resolved at the earliest stages of litigation and present compelling grounds for a stay. *See, e.g.*, *Clarendon Nat'l Ins. Co. v. Glickauf*, No. 18-cv-02549-CMA-NYW, 2019 WL 1897845, at *2 (D. Colo. Feb. 14, 2019) (recognizing that courts in this District "may be more inclined to stay discovery pending the resolution of a Motion to Dismiss impacting immunity or jurisdictional issues"); *Burkitt v. Pomeroy*, No. 15-cv-02386-MSK-KLM, 2016 WL 696107, at *1 (D. Colo. Feb. 22, 2016) ("Questions of jurisdiction and immunity should be resolved at the earliest stages of litigation, so as to conserve the time and resources of the Court and the parties.").

In evaluating whether a stay is warranted, the court may also consider the plaintiff's interests in proceeding expeditiously with the civil action and the potential prejudice to the plaintiff of a delay, the burden on the defendants, and the convenience to the court. *String Cheese Incident, LLC v. Stylus Shows, Inc.*, No. 1:02-cv-01934-LTB-PAC, 2006 WL 894955, at *2 (D. Colo. Mar. 30, 2006). In the end, the decision to stay discovery rests firmly in the sound discretion of the trial court. *See Wang v. Hsu*, 919 F.2d 130, 130 (10th Cir. 1990).

As to Ms. Maser's interest in proceeding expeditiously, when a motion to dismiss raises a jurisdictional issue such as Defendant's motion does in this case, that weighs in favor of a stay. *See, e.g., Lucero v. City of Aurora*, No. 23-cv-00851-GPG-SBP, 2023 WL 5957126, at *2 (D. Colo. Sept. 13, 2023). Under these circumstances, a stay of discovery does not unduly prejudice

Ms. Maser. However, proceeding in the absence of jurisdiction *could* prejudice Ms. Maser; any order this court might issue in the absence of jurisdiction "is no ruling at all." *Colo. Outfitters Ass'n v. Hickenlooper*, 823 F.3d 537, 544 n.5 (10th Cir. 2016) (recognizing that a ruling that assumes the plaintiffs' standing—and by extension assumes the district court's jurisdiction—is necessarily incomplete") (citing *Cunningham v. BHP Petrol. Gr. Brit. PLC*, 427 F.3d 1238, 1245 (10th Cir. 2005) (judgment entered in the absence of jurisdiction is void)). As Defendant is the one requesting the stay of discovery, the stay would not burden it. And the convenience of the court is to stay discovery until Judge Moore rules on this recommendation. Accordingly, Defendant's motion to stay discovery is GRANTED.

In light of this ruling, Defendant's further motion (ECF No. 30) for a protective order from having to respond to Ms. Maser's first sets of discovery requests is moot now that discovery is stayed.

IV. Conclusion

For each of the foregoing reasons, this court RECOMMENDS that the motion to dismiss (ECF No. 15) be granted, and the First Amended Complaint be dismissed without prejudice. The court GRANTS the motion to stay discovery (ECF No. 20) and TERMINATES the motion (ECF No. 30) for protective order as moot.[9]

[9] Rule 72 of the Federal Rules of Civil Procedure provides that within fourteen (14) days after service of a Magistrate Judge's order or recommendation, any party may serve and file written objections with the Clerk of the United States District Court for the District of Colorado. 28 U.S.C. §§ 636(b)(1)(A), (B); Fed. R. Civ. P. 72(a), (b). Failure to make any such objection will result in a waiver of the right to appeal the Magistrate Judge's order or recommendation. *See Sinclair Wyo. Ref. Co. v. A & B Builders, Ltd.*, 989 F.3d 747, 782 (10th Cir. 2021) (firm waiver rule applies to non-dispositive orders); *but see Morales-Fernandez v. INS*, 418 F.3d 1116, 1119, 1122 (10th Cir. 2005) (firm waiver rule does not apply when the interests of justice require

DATED: April 16, 2024

BY THE COURT:

Susan Prose
United States Magistrate Judge

review, including when a "pro se litigant has not been informed of the time period for objecting and the consequences of failing to object").