UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

VICKI STASI, SHANE WHITE, and CRYSTAL GARCIA, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

INMEDIATA HEALTH GROUP CORP.,

Defendant.

Case No.: 19cv2353 JM (LL)

ORDER ON DEFENDANT'S MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINT

Defendant Inmediata Health Group Corp. ("Inmediata") moves under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) to dismiss the First Amended Complaint ("FAC") of Plaintiffs Vicki Stasi, Shane White, and Crystal Garcia. (Doc. No. 17-1.) The motion has been briefed and the court finds it suitable for submission without oral argument in accordance with Civil Local Rule 7.1(d)(1). For the below reasons, Inmediata's motion to dismiss under Rule 12(b)(1) is **DENIED**, and Inmediata's motion to dismiss under Rule 12(b)(6) is **DENIED IN PART** and **GRANTED IN PART**.

I. BACKGROUND

According to Plaintiffs' FAC,[1] Inmediata provides billing and health record software and service solutions to healthcare providers. (FAC ¶¶ 17, 19.) In January of 2019,

[1] Well pled allegations of the FAC are taken as true for purposes of ruling on the motion before the court.

Inmediata first learned it was experiencing a "large data breach" resulting in the "unauthorized acquisition, access, use, or disclosure of unsecured protected health information and personal information" of 1,565,338 individuals. (¶ 2.)[2] Plaintiffs' information was "posted on the Internet" and "searchable and findable by anyone with access to an internet search engine such as Google[.]" (¶ 7.) Plaintiffs' information was "disclosed and released to the entire world – it was viewable online by anyone in the world, printable by anyone in the world, copiable by anyone in the world, and downloadable by anyone in the world." (¶ 8.) The breach did not involve data thieves or hackers. (¶ 9.) Rather, the exposure was "[d]ue to a webpage setting that permitted search engines to index webpages Inmediata uses for business operations[.]" (¶ 7.)

By letter dated April 22, 2019, Inmediata notified Plaintiffs of a "data security incident that may have resulted in the potential disclosure of [their] personal and medical information." (¶ 24; *see also* Doc. Nos. 16-3, 16-4, 16-5.) Inmediata also filed sample "notice of data security incident" letters with various state attorneys general that mirrored the language of the letters sent to Plaintiffs. (¶ 26.) There were two versions of the letter – one for persons whose social security numbers were part of the breach, and another version for persons whose social security numbers were not part of the breach. (¶ 26 n.1.) Plaintiffs received the version for persons whose social security numbers were *not* part of the breach. (*Id.*) The letters stated that "[i]n January 2019, Inmediata became aware that some of its member patients' electronic patient health information was publicly available online as a result of a webpage setting that permitted search engines to index pages that are part of an internal website [Inmediata] use[s] for . . . . business operations." (¶ 27.) The letters also stated that "information potentially impacted by this incident may have included your name, address, date of birth, gender, and medical claim information including dates

[2] Citations to "¶" refer to the FAC.

of service, diagnosis codes, procedure codes and treating physician." (¶ 29.) Inmediata did not offer Plaintiffs fraud insurance or identity monitoring services. (¶ 34.)

On December 9, 2019, Plaintiffs filed a putative class action. On May 5, 2020, Plaintiffs' initial Complaint was dismissed under Rule 12(b)(1). (Doc. No. 15.) On May 19, 2020, Plaintiffs filed their FAC, which included claims for: (1) negligence; (2) breach of contract; (3) unjust enrichment; (4) violation of the California Confidentiality of Medical Information Act; (5) violation of the California Consumer Privacy Act; (6) violation of the California Consumer Records Act; (7) violation of the Minnesota Health Records Act; and (8) invasion of privacy and violation of the California Constitution. (¶¶ 212-324.) Plaintiffs seek to certify a nationwide class consisting of "[a]ll persons . . . . whose [p]ersonal and [m]edical [i]nformation was compromised as a result of the [d]ata [b]reach announced by Inmediata on or around April 24, 2019." (¶ 199.) Plaintiffs alternatively seek to certify statewide classes for California, Minnesota, and Florida. (¶ 200.)

II. LEGAL STANDARDS

A. Rule 12(b)(1)

Rule 12(b)(1) allows a party to move for dismissal of an action based on lack of subject matter jurisdiction. "Dismissal for lack of subject matter jurisdiction is appropriate if the complaint, considered in its entirety, on its face fails to allege facts sufficient to establish subject matter jurisdiction." *In re Dynamic Random Access Memory Antitrust Litig.*, 546 F.3d 981, 984-85 (9th Cir. 2008) (citation omitted). The plaintiff bears the burden of establishing subject matter jurisdiction. *United States v. Orr Water Ditch Co.*, 600 F.3d 1152, 1157 (9th Cir. 2010). If the court finds it lacks subject matter jurisdiction at any time, it must dismiss the action. Fed. R. Civ. P. 12(h)(3). In a facial attack on the pleadings under Rule 12(b)(1), the court accepts the allegations in the complaint as true and draws all reasonable inferences in the plaintiff's favor. *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004).

B. Rule 12(b)(6)

To survive a motion to dismiss under Rule 12(b)(6), the complaint must contain sufficient facts to state a claim for relief that is plausible on its face. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "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." *Id.* at 678. The allegations must be construed in the light most favorable to plaintiff. *Schueneman v. Arena Pharm., Inc.*, 840 F.3d 698, 704 (9th Cir. 2016). While a court must take all factual allegations in the complaint as true, it is "not bound to accept as true a legal conclusion couched as a factual allegation." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678. In resolving the motion, the court does not weigh evidence, evaluate witness credibility, or consider the likelihood that a plaintiff will prevail at trial. *Twombly*, 550 U.S. at 556 ("[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of the facts alleged is improbable, and 'that a recovery is very remote and unlikely[.]'"). Although the court generally cannot consider facts outside the complaint in ruling on a Rule 12(b)(6) motion to dismiss, *Arpin v. Santa Clara Valley Transp. Agency*, 261 F.3d 912, 925 (9th Cir. 2001), it may consider documents that are referenced in the complaint, *No. 84 Employer-Teamster Joint Council Pension Trust Fund v. Am. W. Holding Corp.*, 320 F.3d 920, 925 n.2 (9th Cir. 2003).

III. DISCUSSION

A. Standing

"A suit brought by a plaintiff without Article III standing is not a 'case or controversy,' and an Article III federal court therefore lacks subject matter jurisdiction over the suit." *Cetacean Cmty. v. Bush*, 386 F.3d 1169, 1174 (9th Cir. 2004) (citation omitted). Standing requires the plaintiff to have suffered an injury in fact that is fairly traceable to the challenged conduct of the defendant, and is likely to be redressed by a favorable judicial decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). An injury in fact

is an invasion of a legally protected interest which is concrete and particularized, actual or imminent, and not conjectural or hypothetical. *Id.* at 560.

The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing the elements of Article III jurisdiction. *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990). At the motion to dismiss stage, standing is demonstrated through allegations of specific facts plausibly explaining that standing requirements are met. *Barnum Timber Co. v. Envtl. Prot. Agency*, 633 F.3d 894, 899 (9th Cir. 2011); *see also Warth v. Seldin*, 422 U.S. 490, 518 (1975) ("It is the responsibility of the complainant clearly to allege facts demonstrating that he is a proper party to invoke judicial resolution of the dispute and the exercise of the court's remedial powers."). However, "the court is to 'accept as true all material allegations of the complaint, and . . . . construe the complaint in favor of the complaining party.'" *Levine v. Vilsack*, 587 F.3d 986, 991 (9th Cir. 2009) (quoting *Thomas v. Mundell*, 572 F.3d 756, 760 (9th Cir. 2009)). "[G]eneral factual allegations of injury resulting from the defendant's conduct may suffice," and the court "presume[s] that general allegations embrace those specific facts that are necessary to support the claim." *Lujan*, 504 U.S. at 561 (quotation and alteration omitted). The question of standing is "distinct from the merits" of the plaintiff's claim. *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011); *see also Warth*, 422 U.S. at 500 ("[S]tanding in no way depends on the merits of the plaintiff's contention that particular conduct is illegal[.]").

1. Statutory Standing

Intangible injuries based on violation of a statute can be concrete. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016). "[G]eneral principles" that are "instructive" for assessing whether an intangible injury is concrete include (1) "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," and (2) whether, in Congress' judgment, the intangible harm meets minimum Article III requirements even though it previously did not. *Id.* at 1549. A plaintiff cannot allege "a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of

Article III," but "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact." *Id.*

Plaintiffs argue they sufficiently pled concrete injury by pleading that Inmediata violated the California Confidentiality of Medical Information Act ("CMIA"), CAL. CIV. CODE §§ 56-56.265. (Doc. No. 22 at 10-12.) In support of this argument, Plaintiffs state that CMIA was "enacted to protect people such as Plaintiffs from precisely this sort of long-recognized violation of privacy rights in [confidential medical information]." (*Id.* at 10.) Plaintiffs also state that CMIA was "established to protect concrete privacy interests in medical privacy that go far beyond bare procedural requirements, and [Inmediata's] violations of [CMIA] directly implicate Plaintiffs' interests in those same, concrete, medical privacy rights," (*id.*), and that the California legislature declared the right to privacy "fundamental," (*id.* at 11, 12).[3] As discussed in greater detail below, CMIA prohibits the unauthorized "disclosure" of medical information, the negligent maintenance of medical information, and the negligent "release" of medical information.[4] CAL. CIV. CODE §§ 56.10(a), 56.101(a), 56.36(b). The statute also provides for nominal damages without having to show the plaintiff "suffered or was threatened with actual damages." *Id.* § 56.36(b)(1). Plaintiffs allege that by "posting"[5] their private medical information on the

---

[3] Other than citing *Spokeo II*, Plaintiffs provide almost no support for their statutory standing argument. Plaintiffs do not, for example, discuss the CMIA or its legislative history. Notwithstanding these omissions, the court has an independent obligation to assure Plaintiffs' Article III standing. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180 (2000).

[4] The CMIA applies to health care providers, service plans, and contractors. CAL. CIV. CODE § 56.10(a). Inmediata does not dispute that it is subject to the CMIA.

[5] Plaintiffs do not provide a definition as to what "posting" information on the internet entails. As discussed below, it is not reasonable to infer that Inmediata intentionally posted Plaintiffs' information on the internet. Interpreting the "posting" term in the light most favorable to Plaintiffs, it means that information was made accessible to anyone with an internet connection, intentionally or not.

internet, Inmediata violated CMIA by disclosing the information, negligently failing to preserve its confidentiality, and negligently releasing the information. (¶¶ 269-71.)

a. Ninth Circuit Precedent

At the outset, the alleged intangible injury resulting from "posting" or allowing access to disclosure of Plaintiffs' medical information on the internet in violation of CMIA is, at first blush, just as concrete as the intangible injuries the Ninth Circuit has found to be concrete based on violations of other privacy-related statutes. *See Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1112 (9th Cir. 2020) (alleging Facebook scanned plaintiffs' private messages looking for links to web pages, then allowed third parties to show that the link counted as a "like" on their websites, in violation of the Electronic Communications Privacy Act (ECPA) and the California Invasion of Privacy Act (CIPA)); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020) ("*Facebook Tracking*") (alleging Facebook tracked users' browsing histories when they visited third-party websites, then compiled their browsing histories into profiles which were sold to advertisers in violation of federal and state statutes, including the CIPA; *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1274 (9th Cir. 2019) (alleging Facebook subjected the plaintiffs to facial recognition technology in violation of state biometric privacy statute), *cert. denied*, 140 S. Ct. 937 (2020); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017) (alleging ESPN shared plaintiff's personally identifiable information with a third party in violation of the Video Privacy Protection Act (VPPA)); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (alleging plaintiff received two unsolicited text messages advertising a gym membership in violation of the Telephone Consumer Protection Act (TCPA)); *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1117 (9th Cir. 2017) ("*Spokeo II*") (alleging credit reporting agency published incorrect biographical information about the plaintiff on the internet in violation of procedural requirements of the Fair Credit Reporting Act (FCRA)). For example, it cannot reasonably be argued that the unwanted receipt of text messages advertising a gym membership, annoying as they may be, is a more serious violation of a statutorily protected privacy right than having one's

medical information accessible via the internet for an unknown period of time. Medical information is also just as private and sensitive as the links included in messages sent via Facebook, facial biometric information, and a person's video watching history. *See Campbell*, 951 F.3d at 1112; *Patel*, 932 F.3d at 1274; *Eichenberger*, 876 F.3d at 981. As stated in *Campbell*, "[t]here is no meaningful distinction between the concrete, substantive privacy interests protected by the statutes at issue in *Patel*, *Eichenberger*, and *Van Patten* and the interests protected by the provisions of [the privacy statute] at issue in this case." 951 F.3d at 1118.

Although the Ninth Circuit has found, in near uniformity, that intangible injuries based on alleged violations of privacy-related statutes are sufficiently concrete, Inmediata nonetheless urges the court to follow *Bassett v. ABM Parking Servs., Inc.*, 883 F.3d 776 (9th Cir. 2018). In *Bassett*, the court held the plaintiff did not sufficiently plead a concrete injury by alleging that a parking garage displayed his unredacted credit card expiration date on his receipt, in alleged violation of the FCRA, where the information was not seen by anyone else. *Id.* at 783. The court reasoned, "[w]e need not answer whether a tree falling in the forest makes a sound when no one is there to hear it." *Id.* *Bassett* is distinguishable, however, because in *Bassett* it was known that nobody else saw, or could have seen, the plaintiffs' protected information. Here, Plaintiffs repeatedly allege their information "was viewed by unauthorized persons." (¶¶ 269-271, 277.) Although the basis for Plaintiffs' assertion that their information was actually viewed is sketchy (and, absent ultimate proof, would likely be fatal for Plaintiffs' case in this regard), it is reasonable to infer the information could have been viewed or copied once available on the internet. (*See* ¶¶ 7-8.) In other words, unlike in *Bassett*, the tree falling in the woods question is unavoidable here. Accordingly, even prior to applying the *Spokeo* test, Ninth Circuit precedent strongly supported the concreteness of Plaintiffs' alleged injury resulting from a violation of CMIA.

b. Traditional Harm

Additionally, the harm that results from "posting" medical information on the internet has a close relationship to harm that has traditionally been regarded as providing a

basis for a lawsuit, especially the public disclosure of private facts. *See Forsher v. Bugliosi*, 26 Cal. 3d 792, 808 (1980) (recognizing public disclosure of private facts as a type of invasion of privacy claim); *see also U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."). The Ninth Circuit consistently recognizes that actions based on statutory privacy rights resemble privacy-related claims long available at common law. *See Campbell*, 951 F.3d at 1118 ("The reasons articulated by the legislatures that enacted ECPA and CIPA further indicate that the provisions at issue in this case reflect statutory modernizations of the privacy protections available at common law."); *Patel*, 932 F.3d at 1271-72 (supporting standing based on state biometric data statute because "[p]rivacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts'"); *Eichenberger*, 876 F.3d at 981 (VPPA violations resemble violations of the right to privacy that have "long been actionable at common law," including invasion of privacy, and noting that "privacy torts, such as intrusion of seclusion, do not always require additional consequences to be actionable"); *Van Patten*, 847 F.3d at 1043 (TCPA actions resemble "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts, and the right of privacy is recognized by most states"); *Spokeo II*, 867 F.3d at 1114 (FCRA rights resemble the right to prevent the dissemination of private information and right to bring lawsuits based on the unauthorized disclosure of a person's private information). Accordingly, Plaintiffs' alleged harm is closely related to one traditionally protected at law.

c. Legislative Judgment

Finally, it is reasonable to infer that "posting" Plaintiffs' medical information on the internet constitutes a breach of confidentiality that is precisely the type of harm CMIA was intended to prevent as CMIA expressly provides that actionable injury results from the negligent "release" of medical information regardless of whether the plaintiff "suffered or was threatened with actual damages." *See* CAL. CIV. CODE § 56.36(b). The Ninth Circuit

has repeatedly found the express abdication of the requirement for actual damages in privacy-related statutes supports standing based on violations of those statutes. *See Patel*, 932 F.3d at 1269; *Eichenberger*, 876 F.3d at 981; *Van Patten*, 847 F.3d at 1043.[6]

Although neither party discusses the legislative history of CMIA, the plain language of the statute demonstrates that, in the California legislature's judgment,[7] the provisions of CMIA at issue here are substantive, not procedural. *See also* 1999 Cal. Legis. Serv. Ch. 526 (S.B. 19) ("The bill would . . . . create a right of action to recover damages, as specified, for any individual whose confidential information or records are negligently released and would additionally provide for specified administrative and civil penalties."); *Brown v. Mortensen*, 51 Cal. 4th 1052, 1070-71 (2011) ("[CMIA] is intended to protect the confidentiality of individually identifiable medical information obtained from a patient . . . . [T]he interest protected is an interest in informational privacy[.]") (citation and internal quotation marks omitted); *Heller v. Norcal Mut. Ins. Co.*, 8 Cal. 4th 30, 38 (1994)

---

[6] In *Spokeo*, the Supreme Court emphasized that "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." 136 S. Ct. at 1549. The Court also emphasized, however, that the violation of a statutory right, even a procedural one, "can be sufficient in some circumstances to constitute injury in fact." *Id*. In such cases, "a plaintiff . . . . need not allege any additional harm beyond the one Congress has identified." *Id*.

[7] Although in *Spokeo* the Supreme Court examined the judgment of Congress "because Congress is well positioned to identify intangible harms that meet minimum Article III requirements, 136 S. Ct. at 1549, the Ninth Circuit has applied this line of inquiry to state legislatures and state statutes. *See Facebook Tracking*, 956 F.3d at 598 ("[H]istory and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights[.]"); *Campbell*, 951 F.3d at 1116 ("[W]e are guided in determining concreteness by 'both history and the judgment of Congress,' or the legislature that enacted the statute."); *Patel*, 932 F.3d at 1273 ("The judgment of the Illinois General Assembly . . . . is 'instructive and important' to our standing inquiry[.]").

("[CMIA] was originally enacted in 1979 to provide for the confidentiality of individually identifiable medical information[.]") (citation and internal quotation marks omitted).

As explained in *Eichenberger*, "every violation" of a substantive provision of a privacy-related statute, and "every disclosure" of information protected by that provision, "presents the precise harm and infringes the same privacy interests Congress sought to protect." 876 F.3d at 984; *see also Facebook Tracking*, 956 F.3d at 598 (finding that various privacy-related statutes "codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing"); *Campbell*, 951 F.3d at 1117 ("When . . . . a statutory provision identifies a substantive right that is infringed any time it is violated, a plaintiff bringing a claim under that provision 'need not allege any further harm to have standing.'") (citation omitted); *Patel*, 932 F.3d at 1274 (violation of a biometric privacy statute would "necessarily violate the plaintiffs' substantive privacy interests"). At this early stage in the litigation, nothing in the record suggests Plaintiffs must provide additional proof of the concreteness of their injury beyond their allegations of CMIA violations.[8] Accordingly, Plaintiffs have adequately alleged standing.[9]

///

///

///

---

[8] Because injury in fact exists based on an alleged violation of CMIA, it is not necessary to address Plaintiffs' argument that they also possess standing based on violation of the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1302d.

[9] Courts have consistently found, with little or no discussion, that concrete injuries based on violations of privacy-related statutes are also particularized, fairly traceable (to Inmediata, in this case), and likely to be redressed by a favorable decision. *See, e.g.*, *Campbell*, 951 F.3d at 1116 n.7; *see also Dutta v. State Farm Mut. Auto. Ins. Co.*, 895 F.3d 1166, 1173 (9th Cir. 2018) (injury in fact is the "first and foremost element" of standing). Here, there is no other source of the alleged injury than Inmediata, and the allege injury to Plaintiffs could be redressed by an award of damages or other relief. Also, Inmediata's standing argument does not rest on traceability or redressability issues. Accordingly, Plaintiffs have met their burden of adequately pleading all the elements of standing.

2. Additional Grounds

Plaintiffs also allege they suffered "a privacy injury by having their sensitive medical information disclosed, irrespective of whether or not they subsequently suffered identity fraud, or incurred any mitigation damages." (¶ 284.) The concreteness of this injury is supported by *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019), in which the district court found the plaintiffs' allegation that their "sensitive information was disseminated to third parties in violation of their privacy" was sufficient, by itself, to confer standing, even where no theft or hack of the information occurred and the "sensitive information" did not include social security numbers, financial information, or medical information. The district court rejected Facebook's argument that "a 'bare' privacy violation, without 'credible risk of real-world harm' such as identity theft or other economic consequences, cannot rise to the level of an Article III injury." *Id.* at 786-87. To find otherwise, the court reasoned, would "disregard the importance of privacy in our society, not to mention the historic role of the federal judiciary in protecting it" as recognized by "countless federal laws designed to protect our privacy[.]" *Id.* at 786 (citing, inter alia, HIPAA).

Additionally, at least one district court has found an allegation that the plaintiff "received extensive 'phishing' emails and text messages [and] spent as much as an hour managing the aftermath of the data breach" was sufficient to allege injury in fact. *See Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1035 (N.D. Cal. 2019) ("As consequences of this data breach continue to unfold, so too, will plaintiff's invested time. More phishing e-mails will pile up. At this stage, the time loss alleged suffices."). Here, Plaintiffs allege they spent time "dealing with" and "addressing" issues arising from Inmediata's breach notification. (¶¶ 139, 163, 195.) Plaintiffs also allege they noticed an "increase in spam/phishing" e-mails, calls, or both, from "persons apparently attempting to defraud" them. (¶¶ 136, 157, 192.)

Finally, district courts have found that out-of-pocket expenses are sufficient to confer standing in data breach cases. *See In re Yahoo! Inc. Customer Data Sec. Breach*

Litig., Case No. 16-MD-02752-LHK, 2017 WL 3727318, at *16 (N.D. Cal. Aug. 30, 2017) (listing cases). Here, Plaintiffs allege that Ms. Garcia spent her own money "addressing issues" arising from the breach. (¶ 195.) Accordingly, these cases serve as additional support for the concreteness of Plaintiffs' alleged injuries.[10]

B. Individual Claims

A plaintiff may suffer Article III injury and yet fail to plead a proper cause of action. *Doe v. Chao*, 540 U.S. 614, 624-25 (2004). Inmediata argues that Plaintiffs' individual claims for negligence, breach of contract, unjust enrichment, violation of state privacy statutes, and the California Constitution should be dismissed under Rule 12(b)(6). For the below reasons, this argument is mostly unavailing.

1. Negligence

The elements of a negligence claim under California law are duty, breach, causation, and injury. *Vasilenko v. Grace Family Church*, 3 Cal. 5th 1077, 1083 (2017). Inmediata argues that Plaintiffs' negligence claim is barred by California's economic loss doctrine. (Doc. No. 17-1 at 19-20.) Inmediata also makes arguments with respect to Plaintiffs' allegations of duty, causation, and damages. (*Id.* at 20-21.)

a. Economic Loss Doctrine

Under the economic loss doctrine, "purely economic losses are not recoverable in tort." *NuCal Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) (citation omitted). In the absence of personal injury, physical damage to property, a special relationship between the parties, or some other common law exception to the rule, recovery of purely economic loss for negligence is foreclosed. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 803-04 (1979). Inmediata argues that Plaintiffs' negligence claim is barred by the economic loss doctrine because Plaintiffs do not allege personal injury or property damage.

---

[10] For the same reasons as those stated in the court's initial order granting Inmediata's motion to dismiss, (Doc. No. 15), Plaintiffs arguments with respect to injury based on the future risk of identity theft are unavailing.

(Doc. No. 17-1 at 19-20.) In support of this argument, Inmediata cites *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, Case No.: 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *12 (S.D. Cal. Nov. 3, 2016), in which the district court found the economic loss doctrine barred the plaintiffs' negligence claim because they alleged purely economic damages, i.e. "theft of their credit card information, costs associated with prevention of identity theft, and costs associated with time spent and loss of productivity."

Dugas is not persuasive, however, because even though Plaintiffs allege they lost time responding to Inmediata's breach notification, (*see* ¶¶ 139, 163, 195), they do not necessarily base their allegations on the "costs" of their lost time and lost productivity. Moreover, unlike in *Dugas*, the compromised information here includes medical information, the disclosure of which leads to damages that are not necessarily as "economic" as those resulting from the theft of credit card information and social security numbers. Indeed, Plaintiffs allege they suffered "a privacy injury by having their sensitive medical information disclosed, irrespective of whether or not they subsequently suffered identity fraud, or incurred any mitigation damages." (¶ 284.) Plus, Plaintiffs allege they noticed an increase in spam/phishing e-mails and/or calls, (¶¶ 136, 157, 192), which is harm that is also not necessarily "economic" in nature. Accordingly, at least two district court cases, with facts more similar to the instant case than those in *Dugas*, found that time spent responding to a data breach is a non-economic injury, that when alleged to support a negligence claim, defeats an economic loss doctrine argument. *See Solara*, 2020 WL 2214152, at *4 (involving theft of medical information); *Bass*, 394 F. Supp. 3d at 1039 (involving the hack of non-financial personal information, the only alleged misuse of which was spam e-mails). Other than citing *Dugas*, Inmediata does not meaningfully address these alleged injuries in its motion to dismiss Plaintiffs' negligence claim.[11]

---

[11] In its reply, Inmediata merely states, without citing any authority, that "the loss of time does not meet the requirement that there must be bodily injury or property damage." (Doc. No. 23 at 11.)

The applicability of the economic loss doctrine is also questionable given that Plaintiffs and Inmediata were not in privity of contract, there was no commercial activity between Plaintiffs and Inmediata that went awry, and the case does not involve a defective product or services resulting in mere "disappointed expectations." *See Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) ("The economic loss rule requires a purchaser to recover in contract for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise. Quite simply, the economic loss rule prevents the law of contract and the law of tort from dissolving one into the other.") (internal quotation marks and alteration omitted); *see also Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 880 (9th Cir. 2007) (finding the economic loss doctrine did not apply because appellants' tort claim was not a "mere contract claim cloaked in the language of tort"); *Dugas*, 2016 WL 6523428, at *1 (involving dispute between parties in privity of contract).

Finally, as discussed above, the statutory protection afforded to medical information is rooted in common law duties traditionally serving as the basis for lawsuits, including the duty not to publicly disclose private facts. Therefore, to the extent the economic loss rule does apply, it is plausible a common law exception to the rule also applies. (*See* Doc. No. 22 at 27-28.) Accordingly, at this stage in the litigation, the economic loss doctrine does not defeat Plaintiffs' negligence claim.

b. Duty and Breach

Inmediata argues that Plaintiffs have not alleged a common law duty because "it is not plausible to suggest Inmediata could foresee that an errant web page setting would result in identity theft or fraudulent transactions using stolen patient data." (Doc. No. 17-1 at 20.) This is not an accurate description of Plaintiffs' allegations. In their FAC, Plaintiffs repeatedly, and in a variety of ways, allege that Inmediata owed them a duty to safeguard their personal and medical information as consistent with medical privacy statutes and industry standards. (¶¶ 81-87, 218-226, 231.) Emphatically, the issue here is *not* foreseeability of harm.

District courts have found comparable allegations sufficient to survive motions to dismiss negligence claims. *See Castillo v. Seagate Tech., LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *2 (N.D. Cal. Sept. 14, 2016) (alleging employer had duty to reasonably protect employees' information); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *3 (C.D. Cal. June 15, 2015) (alleging employer owed employees a duty to implement and maintain adequate security measures to safeguard their personal information); *see also Facebook*, 402 F. Supp. 3d at 799 (finding a duty because "Facebook had a responsibility to handle its users' sensitive information with care"); *Bass*, 394 F. Supp. 3d at 1039 (alleging Facebook failed to comply with industry data-security standards).

Inmediata cites no data breach case in which the court found the plaintiffs failed to adequately allege duty. Instead, Inmediata argues that without a "special relationship," it owed no duty to Plaintiffs to protect their information from thieves and hackers.[12] (Doc. No. 17-1 at 20.) Inmediata provides no support, however, for its argument that no special relationship exists between a company that possesses peoples' personal and medical information and those people. In *Castillo*, a case upon which Inmediata relies, the court found an employer had a duty to protect the personal information it possessed regarding not only its employees and former employees, but also their spouses and dependents. 2015 WL 3916744, at *3. In reaching this conclusion, the court applied the factors identified in *Rowland v. Christian*, 69 Cal. 2d 108, 113 (1968), which the district court described as:

> (1) the foreseeability of the harm to the plaintiff; (2) the degree of certainty that the plaintiff suffered injury; (3) the closeness of the connection between the defendant's conduct and the injury suffered; (4) the moral blame attached to the defendant's conduct; (5) the policy of preventing future harm; and (6) the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for

[12] For this reason, Inmediata's argument concerning a common law duty appears to be aimed more towards Inmediata's economic loss doctrine argument rather than attacking the duty element of Plaintiffs' negligence claim.

> breach and the availability, cost, and prevalence of insurance for the risk involved.

Id.

Applied here, these factors weigh in favor of the plausibility that Inmediata owed a duty to protect Plaintiffs' information despite the fact that Plaintiffs were not Inmediata's customers or otherwise in privity with Inmediata. As noted above, Plaintiffs allege they lost time responding to Inmediata's breach notification, (¶¶ 139, 163, 195), and that they noticed an increase in spam/phishing e-mails and/or calls, (¶¶ 136, 157, 192). Plaintiffs also allege that Ms. Garcia spent her own money. (¶ 195.) It is foreseeable that these alleged harms would result from posting Plaintiffs' personal and medical information on the internet. While the chance that Plaintiffs will actually suffer identity theft is unknown[13] and has likely decreased over time, it is reasonable to infer that persons whose information was compromised in such a manner would, at the very least, spend some time and/or effort to detect or prevent identity theft. It can also reasonably be said that Inmediata bears some "moral" blame for failing to protect medical information concerning persons who were likely unaware that Inmediata possessed their medical information in the first place. (*See* ¶ 158 (alleging Mr. White spent hours "attempting to determine how he is connected to Inmediata and how his information came into the possession of Inmediata.").) Additionally, imposing a common law duty on companies that possess personal and medical information to safeguard that information further promotes a policy, statutorily recognized, of preventing identity theft and protecting the confidentiality of medical information. Finally, the burden of imposing a common law duty to protect medical and personal information is not likely high given that both state and federal law already require such protection, and, in the case of state law, already allows for a private right of action.

---

[13] As discussed below, it is also far from reasonably certain Mr. White's alleged identity theft was the result of this data breach.

In the context of this case, the burden appears especially light given Inmediata's position that an "errant webpage setting" was the culprit. (Doc. No. 17-1 at 20.)

Overall, it is reasonably foreseeable that a company that possesses medical information for thousands of people would cause those people time and effort upon learning that information had been freely accessible on the internet. *See Bass*, 394 F. Supp. 3d at 1039 (finding the *Rowland* test supported the assertion that Facebook owed its users a duty of care because, inter alia, "[t]he lack of reasonable care in the handling of personal information can foreseeably harm the individuals providing the information," including harm in the form of lost time). Accordingly, Plaintiffs plausibly allege breach of duty.

c. Causation

Inmediata further argues that Plaintiffs fail to sufficiently allege causation because they do not allege an unauthorized person actually viewed or downloaded their data, or that they experienced identity theft, fraudulent charges, or any other legally cognizable harm. (Doc. No. 17-1 at 21.) The only support Inmediata provides for this argument is a citation to *Castillo*, in which the plaintiff employees all suffered identity theft in the form of falsely filed tax returns. 2016 WL 9280242, at *2. The district court found that causation was not adequately pled for one of the named plaintiffs because she conceded that her information had been compromised during a previous, unrelated data breach. *Id.* at *4. The court stated, "[t]o create a reasonable inference the [defendant's] data breach caused the [false tax] filing, [the plaintiff] should plead more particular facts connecting the two events, such as the temporal relationship between the breach and the false filing, or the similarities between the false filing in her name and the filings in the names of other [persons whose data was breached]." *Id.*

This argument is persuasive with respect to the allegation that Plaintiff White actually experienced identity theft. In addition to the injuries already discussed above, Plaintiffs allege that, approximately nine months after Inmediata first learned of the data breach, Mr. White suffered $600 in fraudulent charges on his credit card. (¶¶ 159-162.) Because he used the card to pay for healthcare, Plaintiffs allege that Mr. White "believes

Inmediata was the source of his breached credit card information." (¶ 162.) As was the case in *Castillo*, however, Plaintiffs acknowledge that Mr. White received a data breach notification resulting from a 2017 data breach involving Equifax. (¶ 161). Additionally, Plaintiffs acknowledge that Inmediata specifically informed them that "financial information" was "not involved." (¶ 30.) Plaintiffs nonetheless state they "do not accept this as an accurate statement" because the letter they received in Inmediata's letter advised them to "keep[] a close eye on your credit card activity." (*Id.*) However, Inmediata's letter, which is attached to the FAC, contains no such language and does not reference credit card information. Additionally, Plaintiffs acknowledge that Inmediata specifically informed them "[b]ased on the investigation, we have no evidence that any files were copied or saved" and "we have not discovered any evidence that any information that may be involved in this incident has been misused." (*See* Doc. No. 16-4 at 2.) For these reasons, Plaintiffs cannot allege a plausible negligence claim based on Mr. White's allegation that he actually experienced identity theft. As discussed above, however, it is plausible the lost time and increase in spam/phishing Plaintiffs allegedly suffered was caused by the alleged breach of Inmediata's duty to protect their personal and medical information, and Inmediata does not argue otherwise.

d. Damages

i. Lost Time

As noted above, Plaintiffs allege they suffered damages in the form of lost time. Specifically, Plaintiffs allege that Ms. Stasi spent time "trying to make sure she has not and does not become further victimized because of the Data Breach," (¶ 139), Mr. White spent time "dealing with the aftermath of the Data Breach," (¶ 163), and Ms. Garcia spent time "addressing issues arising from the Data Breach," (¶ 195). Plaintiffs also allege that, since early 2019 when Inmediata first became aware of the breach, they noticed an "increase in spam/phishing" e-mails, calls, or both, from "persons apparently attempting to defraud" them. (¶¶ 136, 157, 192.)

Generally, it can be inferred that theft of social security numbers, financial information, and medical information is primarily financially motivated and realized through identity theft or other forms of fraud. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."); *Bass*, 394 F. Supp. 3d at 1035 ("It is not too great a leap to assume . . . . that [hackers'] goal in targeting and taking . . . . information [is] to commit further fraud and identity theft."). Accordingly, the Ninth Circuit has held that theft of information that can be used to commit identity theft causes an injury to victims for standing purposes based on the future threat of identity theft regardless of whether the named plaintiffs actually suffered identity theft. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018), *cert. denied sub nom. Zappos.com, Inc. v. Stevens*, 139 S. Ct. 1373 (2019); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010).[14]

The instant case is not, however, the typical data breach case because it does not involve the theft or hack of information that courts have recognized as enabling identity theft, such as financial information or social security numbers, and there are no plausible allegations that Plaintiffs actually suffered identity theft resulting from the alleged breach. Rather, at this stage, the case involves allegations that Plaintiffs' medical information, including diagnosis codes and treating physicians, was posted on the most publicly accessible forum in the world for an unknown period of time. In other words, the interest

---

[14] As this court previously found, in both *Krottner* and *Zappos* the Ninth Circuit held that misuse of the named plaintiffs' information was not necessarily required for standing purposes, but the court nonetheless relied on allegations of actual misuse of others victims' information to find standing. *See Krottner*, 628 F.3d at 1142 (noting that one of the plaintiffs alleged that someone unsuccessfully attempted to open a bank account in his name); *Zappos*, 888 F.3d at 1027-28 (noting that some non-parties had their accounts commandeered and suffered financial losses, and that two plaintiffs had their e-mail accounts taken over).

in the confidentiality of medical information is not, as Inmediata apparently presumes, necessarily tied to the risk of identity theft. Accordingly, although some cases have found that when information capable of being used to commit identity theft is stolen, it must also be misused in order to find injury, *see, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012), the facts here are different. Although Plaintiffs do not provide great detail in describing how they expended time and effort after receiving Inmediata's breach notification, it is reasonable to infer that upon receiving notice of the breach they responded by ensuring: (1) that their medical information was no longer accessible via the internet; (2) that their information did not reappear on the internet; and/or (3) they had not, and would not, become victims of identity theft. "Increased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by other courts to be specific, concrete, and non-speculative." *Solara*, 2020 WL 2214152, at *4 (declining to dismiss negligence claim under Rule 12(b)(6) on this ground); *see also Adkins*, 424 F. Supp. 3d at 692 (time lost responding to a data breach establishes a harm for standing purposes); *but see Corona*, 2015 WL 3916744, at *4 (finding, without discussion, that "general allegations of lost time are too speculative to constitute cognizable injury" in case involving an alleged hack, theft, and misuse of employee financial and medical information). It is also reasonable to infer that the receipt of alleged spam/phishing e-mails and/or calls cost Plaintiffs some of their time. Even though Plaintiffs do not allege that their e-mail addresses or phone numbers were included in the information that was compromised, it would nonetheless be reasonable for them to be curious about spam/phishing contacts they received after being informed of the data breach. *See Bass*, 394 F. Supp. 3d at 1035 (finding that time spent "sorting through a few dozen e-mails," though de minimis, is a sufficient injury for standing purposes because "[as] consequences of [the alleged] data breach continue to unfold, so too, will plaintiff's invested time"). Accordingly, at this early stage in litigation, Plaintiffs allege plausible damages in the form of lost time, and Inmediata has not met its burden of showing otherwise.

ii. Lost Money

Plaintiffs also allege that Ms. Garcia "spent her own money . . . . addressing issues arising from the Data Breach." (¶ 195.) Plaintiffs do not specify what Ms. Garcia spent her money on, or what "issues" she "addressed." As pointed out by Inmediata, Plaintiffs do not allege they actually purchased credit monitoring services. (*See* Doc. No. 17-1 at 17.) Construing this allegation in the light most favorable to Plaintiffs, however, it is reasonable to infer at this stage in litigation that Ms. Garcia spent her money on some form of identity theft protection. (*See* ¶¶ 193-94 (alleging she placed credit freezes on her credit reports in order to detect potential identity theft and fraudulent activity, and now engages in monthly monitoring of her credit and her bank accounts); *see also* Doc. No. 22 at 25 ("Plaintiffs engaged credit monitoring services as a result of the . . . . risk of future identity theft.").)

In data breach cases involving negligence claims, district courts have found it sufficient to allege out-of-pocket expenses in purchasing identity theft protection services to show damages. *See Castillo*, 2016 WL 9280242, at *4 ("Those who have incurred such out-of-pocket expenses [such as purchasing identity protection services] have pleaded cognizable injuries[.]"); *Corona*, 2015 WL 3916744, at *4 (finding the same by analogizing costs associated with identity theft protection to those resulting from exposure to toxic chemicals); *see also Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1233 (D. Nev. 2020) ("[T]angible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as damages."); *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 695 (N.D. Cal. 2019) (denying class certification because the plaintiff "never paid any money as a result of this data breach" and "never purchased any credit monitoring service"); *Yahoo*, 2017 WL 3727318, at *16 (money spent to monitor credit and prevent future identity theft is sufficient injury for standing purposes).

These cases may be distinguishable because they involve far more serious data breaches than what Plaintiffs allege here. *See Castillo*, 2016 WL 9280242, at *2 (defendant employer released all of its employees' tax information in response to a phishing scam,

after which the plaintiff employees all suffered identity theft in the form of fraudulently filed tax returns); *Corona*, 2015 WL 3916744, at *4 (hackers stole, and traded on the internet, social security numbers, financial information, medical information, home and e-mail addresses, and visa and passport numbers). However, in arguing that Plaintiffs failed to state a claim for negligence under Rule 12(b)(6), Inmediata does not argue these cases are distinguishable. In fact, Inmediata does not specifically address the allegation that Ms. Garcia spent her own money.

Instead, Inmediata argues, as it did in its standing argument, under California law Plaintiffs' allegation that they took steps to protect against possible future risk of identity theft is insufficient.[15] (Doc. No. 17-1 at 21.) The only support Inmediata provides for this argument is a citation to *Corona*, 2015 WL 3916744. In *Corona*, however, the district court did not find that the plaintiffs failed to adequately allege injury, either for standing or Rule 12(b)(6) purposes. To the contrary, with respect to the *Corona* plaintiffs' negligence claim, the court found they adequately alleged a cognizable injury "by way of costs relating to credit monitoring, identity theft protection, and penalties." 2015 WL 3916744, at *5. Accordingly, Plaintiffs sufficiently allege that Ms. Garcia suffered damages in the form of lost money.

e. Negligence Per Se

In their FAC, Plaintiffs allege they are entitled to an evidentiary presumption of negligence per se based on violations of various statutes, including CMIA. (¶ 229.) Under California law, Inmediata's failure to exercise due care is presumed if Plaintiffs sufficiently allege that: (1) Inmediata violated a statute or regulation; (2) the violation was the proximate cause of Plaintiffs' injury; (3) the injury resulted from an occurrence, the nature

---

[15] Inmediata's reference to its argument against Plaintiffs' standing in support of its argument against Plaintiffs' negligence claims is not particularly helpful given that Plaintiffs bear the burden of showing standing while Inmediata bears the burden of showing that Plaintiffs failed to state their claim for negligence under Rule 12(b)(6).

of which the statute or regulation was designed to prevent; and (4) the person suffering the injury was one of the class of persons for whose protection the statute or regulation was adopted. CAL. EVID. CODE § 669. District courts have relied on allegations of negligence per se to deny Rule 12(b)(6) motions to dismiss. *See, e.g.*, *Harris v. Burlington N. Santa Fe R.R.*, No. 17-cv-2433-BAS-JLB, 2013 WL 12122668, at *2 (C.D. Cal. July 12, 2013). The negligence per se doctrine does not, however, obviate the need for Plaintiffs to show a viable and independent duty. *See Nikoopour v. Ocwen Loan Servicing, LLC*, Case No.: 17cv2015-MMA (WVG), 2018 WL 1035210, at *7 (S.D. Cal. Feb. 23, 2018) (citations omitted).

As discussed below, Plaintiffs plead a plausible violation of CMIA, which provides for nominal damages even if Plaintiff did not suffer actual damages. *See* CAL. CIV. CODE § 56.36(b)(1). Also, it is reasonable, at this stage in the litigation, that Plaintiffs' alleged injuries resulting from the "posting" of their medical information on the internet are the injuries the statute was intended to prevent, and that Plaintiffs, as persons who initially provided the confidential medical information that Inmediata possessed, are within the class of persons for whose protection the statute was adopted. Accordingly, to the extent the instant negligence claim is distinguishable from those in data breach cases involving a theft or hack of social security numbers or financial information, this distinction is counter-buttressed by this case involving confidential medical information protected by statute. Accordingly, the negligence per se doctrine supports the plausibility of Plaintiffs' negligence claim.

2. Breach of Contract

a. Third Party Beneficiaries

Plaintiffs allege, based on information and belief, that they are intended third party beneficiaries of contracts between Inmediata and its customers that require Inmediata to take appropriate steps to safeguard Plaintiffs' information. (¶¶ 248-49.) Inmediata argues these allegations are conclusory and not supported by any facts, such as specific contract language or the identity of the parties to the contracts. (Doc. No. 17-1 at 24-25.)

The standard to achieve third party beneficiary status is a high one. *See Goonewardene v. ADP, LLC*, 6 Cal. 5th 817, 821 (2019) (a motivating purpose of the contracting parties must be to provide a benefit to the third party); *see also Cummings v. Cenergy Int'l Servs., LLC*, 271 F. Supp. 3d 1182, 1188 (E.D. Cal. 2017) ("It is well settled . . . . that enforcement of a contract by persons who are only incidentally or remotely benefitted by it is not permitted."). Moreover, the alleged contractual terms, if they exist, likely refer to Inmediata's pre-existing statutory duties to safeguard the medical information in its possession. *See In re Anthem, Inc. Data Breach Litig.*, Case No. 15-MD-02617-LHK, 2016 WL 3029783, at *20 (N.D. Cal. May 27, 2016) ("A breach of contract claim based solely upon a pre-existing legal obligation to comply with HIPAA can not survive dismissal."). Additionally, district courts in data breach cases have dismissed breach of contract claims for failure to identify the specific language in the contract that was breached. *See, e.g., Hassan v. Facebook, Inc.*, Case No. 19-cv-01003-JST, 2019 WL 3302721, at *3 (N.D. Cal. July 23, 2019).

Based on the above, Plaintiffs' breach of contract claim is tenuous at best. At this stage in the litigation, however, Plaintiffs plausibly allege they are third party beneficiaries, and Plaintiffs' allegations are sufficiently factual to give fair notice and to enable Inmediata to defend itself effectively. *See Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). Although Plaintiffs do not provide specific contract terms, Plaintiffs allege the substance of the relevant terms. *See McKell v. Washington Mut., Inc.*, 142 Cal. App. 4th 1457, 1489 (2006); *see also Summit Estate, Inc. v. Cigna Healthcare of California, Inc.*, Case No. 17-CV-03871-LHK, 2017 WL 4517111, at *4 (N.D. Cal. Oct. 10, 2017). Moreover, without discovery, it is not clear what more Plaintiffs could plead, or what more Inmediata would need to be able to defend against Plaintiffs' claims that they are third party beneficiaries of Inmediata's contracts. In the early stages of litigation, plaintiffs may base their allegations, even jurisdictional ones, on information and belief when the allegations include facts that are primarily within the defendant's knowledge. *Carolina Cas. Ins. Co. v. Team Equip., Inc.*, 741 F.3d 1082, 1087 (9th Cir. 2014); *see also Park v. Thompson*, 851 F.3d 910, 928

(9th Cir. 2017) (*Iqbal*/*Twombly* plausibility standard does not prevent a plaintiff from pleading facts alleged upon information and belief). Accordingly, Plaintiffs' allegations that contracts exist that contain terms protecting their information are sufficient to allege a breach of contract claim based on a third party beneficiary theory.

b. Damages

Inmediata argues that Plaintiffs have not adequately pled damages because they do not plead (1) they were victims of identity theft, except for the "wildly speculative" allegations of Mr. White regarding unknown charges to his credit card, or (2) they paid for credit monitoring services. (Doc. No. 17-1 at 22.) As Inmediata points out, some district courts have found that fear of future identity theft is too speculative to support damages in a breach of contract claim. *See*, *Svenson v. Google Inc.*, 65 F. Supp. 3d 717, 724-25 (N.D. Cal. 2014); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 918 (N.D. Cal. 2009), *aff'd*, 380 F. App'x 689 (9th Cir. 2010). Additionally, the standard for damages under California contract law may be higher than that for negligence claims. *See Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000) (plaintiffs must show appreciable and actual damage that is not nominal, speculative, or based on fear of future harm). Also, as discussed above, Inmediata is correct that Mr. White's allegations regarding the fraudulent charges on his credit card are unreasonably speculative.

However, the cases dismissing breach of contract claims for lack of plausible damages did not involve medical information that was allegedly posted on the internet. Moreover, Inmediata does not argue that breach of contract claims have substantively different standards for damages than negligence claims. Also, Inmediata is incorrect that Plaintiffs' fail to allege they paid for credit monitoring services. Rather, as discussed above, Plaintiffs allege that Ms. Garcia "spent her own money . . . . addressing issues arising from the Data Breach," (¶ 195), and this is sufficient to infer that she spent the money on some form of identity theft protection.

Additionally, other district courts have found, or at least suggested, that an alleged invasion of privacy is per se sufficient to show damages in a breach of contract claim. *See*

Facebook, 402 F. Supp. 3d at 802 ("[U]nder California law even those plaintiffs [who did not suffer measurable compensatory damages] may recover nominal damages."); *Solara*, 2020 WL 2214152, at *5 ("The dissemination of one's personal information can satisfy the damages element of a breach of contract claim."); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 834 (N.D. Cal. 2020) ("[T]he detriment Plaintiffs say they suffered was an invasion of their privacy. Plaintiffs are entitled to seek compensatory damages or perhaps nominal damages for such harm."); *see also Facebook Tracking*, 956 F.3d 589, 598 (9th Cir. 2020) (finding that plaintiffs had standing to bring claims for breach of contract by adequately alleging "privacy harms"). Accordingly, Plaintiffs sufficiently plead damages in their breach of contract claim.

3. Unjust Enrichment

Inmediata argues, and Plaintiffs concede, that they have not pled a plausible claim for unjust enrichment under California law. (*See* Doc. Nos. 17-1 at 24-25; 22 at 30 n.2.) Accordingly, Plaintiffs fail to state a plausible claim for unjust enrichment under California law. Plaintiffs nonetheless argue that Inmediata does not challenge their unjust enrichment claims under Florida and Minnesota law. (Doc. No. 22 at 30.) In their FAC, however, Plaintiffs do not list their purported claims for unjust enrichment under Florida or Minnesota law as separate claims, and Plaintiffs make only passing reference to Florida and Minnesota law. (*See* ¶¶ 226-27.) To the extent that Plaintiffs actually and sufficiently allege unjust enrichment under Florida and Minnesota law, those claims survive because they are not challenged.

4. California Confidentiality of Medical Information Act

Inmediata argues that Plaintiffs fail to state a plausible violation of CMIA, CAL. CIV. CODE §§ 56-56.265, because they do not allege facts suggesting that an unauthorized person "actually viewed" their confidential information. (Doc. No. 17-1 at 26.) As noted above, Plaintiffs allege that by posting their medical information on the internet, Inmediata violated multiple provisions of CMIA, including the first sentence of section 56.10(a) (prohibiting "disclosure"), the first sentence of section 56.101(a) (establishing a duty to

"preserve confidentiality"), and section 56.36(b) (allowing a private right of action for "negligent release").[16] (¶¶ 269-71, 277.) As a result, Plaintiffs seek actual and nominal damages. (¶ 281.)

a. Section 56.10(a)

Under California law, in order to plead a violation of section 56.10(a), which mandates that health care providers and contractors shall not "disclose" medical information, the plaintiff must plead an "affirmative communicative act" by the defendant, which does not occur if the information is stolen. *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1556 (2014); *see also Regents of Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 564 (2013) ("disclose" under CMIA means an "affirmative act of communication"). Plaintiffs allege that Inmediata employees "posted" their information on the internet, and that "posting" is an affirmative communicative act. (¶¶ 269-71.)

Here, it is reasonable to infer that some affirmative act by Inmediata caused the "errant webpage setting" that allegedly made Plaintiffs' information accessible via the internet. However, while intentionally posting something on the internet is inherently communicative, Plaintiffs do not allege that Inmediata intentionally[17] posted their information, or that whatever affirmative act might have caused their information to

---

[16] Plaintiffs also allege that Inmediata violated: (1) sections 56.101(b)(1) related to its electronic health record system; (2) section 56.26(a) by using their information in a manner not reasonably necessary in connection with the administration or maintenance of payment for health care services program; (3) section 56.10(d) by intentionally using their information for a purpose not necessary to provide health care services; and (4) section 56.10(e) by disclosing their information to persons or entities not engaged in providing direct health care services. (¶273-276, 278-79.) Inmediata does not argue that Plaintiffs have failed to state a claim with respect to these provisions.

[17] Although Plaintiffs allege that Inmediata "intentionally shared, sold, used for marketing, or otherwise used" their information "for a purpose not necessary to provide health care services," (¶ 278), this is merely a recitation of the elements of section 56.10(d) of the CMIA. The same is true where Plaintiffs use the word "intent" to allege fraud. (See ¶ 304.)

become accessible via the internet was done with the intent to communicate that information. Based on the meaning of "disclose" as defined in *Sutter* and *Regents*, Plaintiffs have not pled a plausible violation of section 56.10(a) of CMIA.

b. Sections 56.101(a) and 56.36(b)

The first sentence of section 56.101(a) in CMIA provides that every health care provider and contractor "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein."[18] CAL. CIV. CODE § 55.101(a). The second sentence provides that any health care provider or contractor "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Section 56.36(b) provides, in turn, that nominal and actual damages are available when information is "negligently released."[19] § 56.36(b). In *Regents*, the court held that in order to plead a violation of sections 56.101(a) and 56.36(b), the plaintiff does *not* need to plead an affirmative communicative act. 220 Cal. App. 4th at 553-54; *see also Corona*, 2015

---

[18] Unlike other provisions of the CMIA, however, this provision does not state that damages are available for violations. *See Lu v. Hawaiian Gardens Casino, Inc.*, 50 Cal. 4th 592, 596 (2010) ("A violation of a state statute does not necessarily give rise to a private cause of action."). As recognized in *Regents*, to allow claims based on violation of this provision alone would allow persons other than the patient to bring suit. *Regents*, 220 Cal. App. 4th at 563.

[19] On its face, the statute is unclear as to whether, in order to recover actual or nominal damages for, say, "negligent maintenance" of information, the plaintiff must also show that the information was "negligently released." In *Regents*, however, the court clarified that in order to sufficiently plead actual or nominal damages under CMIA, it is insufficient for the plaintiff to plead, under the second sentence of section 56.101(a), that the defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information. 220 Cal. App. 4th at 554. Rather, the plaintiff must also plead that their information was negligently "released" under section 56.36(b). *Id.*

WL 3916744, at *7; *Sutter*, 227 Cal. App. 4th 1554 (assuming the same). The court also held, however, that plaintiffs must plead that "negligence result[ed] in unauthorized or wrongful access to the information," i.e. that the information was "improperly viewed or otherwise accessed."[20] *Id.* at 554. Similarly, in *Sutter*, the court held that "[n]o breach of confidentiality takes place until an unauthorized person views the medical information." 227 Cal. App. 4th at 1557. The *Sutter* court stated, "[t]hat the records have changed possession even in an unauthorized manner does not mean they have been exposed to the view of an unauthorized person." *Id.* at 1558.

Here, *Regents* and *Sutter* do not preclude Plaintiffs' remaining CMIA claims because the Plaintiffs repeatedly allege their information "was viewed by unauthorized persons."[21] (¶¶ 269-271, 277.) The lack of allegations that the plaintiffs' information was actually viewed was crucial to the courts' decisions in *Regents* and *Sutter*. *See Sutter*, 227 Cal. App. 4th at 1555 ("[T]he main pleading problem for the plaintiffs in this case and in *Regents* is the same: there is no allegation that the medical information was viewed by an unauthorized person."). Additionally, in both *Regents* and *Sutter*, the stolen data was password protected and/or encrypted. *See Sutter*, 227 Cal. App. 4th at 1555. The same cannot be said for information that is posted and accessible on the internet.[22] Given the

---

[20] The court found that pleading negligent maintenance and loss of possession based on the theft of the data is insufficient to state a claim under sections 56.101 and 56.36(b). *Regents*, 220 Cal. App. 4th at 569-70.

[21] Strangely, Inmediata argues that "Plaintiffs do not even allege an unauthorized person actually viewed or downloaded their data." (Doc. No. 17-1 at 21.)

[22] In cases where the plaintiffs allege their information was stolen and actually misused, district courts have declined to dismiss CMIA claims under Rule 12(b)(6). *See In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1189, 1202 (D. Or. 2016) (hack); *Corona*, 2015 WL 3916744 (hack), at *7; *Falkenberg v. Alere Home Monitoring, Inc.*, Case No. 13-cv-00341-JST, 2015 WL 800378, at *4 (N.D. Cal. Feb. 23, 2015) (theft of a password protected laptop). Here, only one of the Plaintiffs alleges actual identity theft, and it is a weak allegation at that. This weakness is counter-balanced,

relatively clear holdings in *Regents* and *Sutter*, Plaintiffs' allegation that their information was actually viewed could be read, of course, as a threadbare and conclusory recital of an essential element to their CMIA claim. When read in the light most favorable to Plaintiffs, however, the allegation that their information was actually viewed is at least somewhat factual.

Additionally, one court in this district recently found it sufficient for plaintiffs to plead that they received a letter stating their medical information was exposed in a data breach, and the only evidence that it had actually been viewed was an increase in medical-related spam e-mails and phone calls. *See Solara*, 2020 WL 2214152, at *7. The court found these allegations sufficient to infer the plaintiffs' medical information was viewed by an unauthorized party, even though the plaintiffs did not specifically allege that it was. *Id.* As an alternative to their allegation that their information was actually viewed, Plaintiffs repeatedly assert that they reasonably believe, and it should be inferred or rebuttably presumed, that their information was actually viewed. (*See, e.g.*, ¶¶ 46-48.) Given that Plaintiffs allege that Inmediata posted their information on the internet, making it searchable, findable, viewable, printable, copiable, and downloadable by anyone in the world with an internet connection, (¶¶ 7-8), it can be reasonably inferred that someone viewed it. Ultimately, it may be that Plaintiffs' allegation that their information was actually viewed while it was accessible on the internet will prove to be unsubstantiated. At this early stage in the litigation, however, Plaintiffs allege a plausible claim based on violations of sections 56.101(a) and 56.36(b) of CMIA, and Inmediata has not met its burden of showing otherwise.

---

however, because the Plaintiffs information was allegedly accessible on the most public forum in the world, and not just to the thief or thieves. And again, Inmediata does not argue to any convincing degree that cases involving theft or hacking are distinguishable. Additionally, when suing for nominal damages under CMIA, plaintiffs do not have to prove they "suffered or [were] threatened with actual damages." CAL. CIV. CODE § 56.36(b)(1).

5. California Consumer Privacy Act

Inmediata argues that Plaintiffs fail to state a claim for violation of the California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.150(a), because (1) Plaintiffs merely allege that it should be inferred or rebuttably presumed that their information was accessed by an unauthorized individual, which is insufficient to allege theft of or "unauthorized access" to their personal information, and (2) Plaintiffs allege violation of the CCPA based on the exposure of both their personal and medical information, but the CCPA does not apply to medical information governed by CMIA. (Doc. No. 17-1 at 27.)

As discussed above, Plaintiffs do not merely allege that it should be inferred or rebuttably presumed that their information was accessed by an unauthorized individual. Plaintiffs repeatedly allege that their information "was viewed by unauthorized persons." (*See, e.g.*, ¶¶ 269-271, 277.) Moreover, Inmediata does not point to any authority requiring Plaintiffs to plead theft or unauthorized access in order to plead a plausible violation of the CCPA. The CCPA provides a private right of action for actual or statutory damages to "[a]ny consumer whose nonencrypted and nonredacted personal information . . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information[.]" *Id.* § 1798.150(a). Plaintiffs argue, and Inmediata does not dispute, that the facts alleged in the FAC that Plaintiffs' personal and medical information were accessible via the internet, constitutes a "disclosure" under the CCPA. (Doc. No. 22 at 22-23.) Further, although Inmediata is correct that the CCPA does not apply to medical information governed by CMIA, § 1798.145(c)(1)(A), Inmediata does not address the non-medical information that it admits was accessible on the internet. Accordingly, at this early stage in the litigation, Plaintiffs allege a plausible claim based on violation of the CCPA, and Inmediata has not met its burden of showing otherwise.

6. California Consumer Records Act

Plaintiffs allege that by taking 81 days to inform them of the data breach, Inmediata acted with unreasonable delay in violation of the California Customer Records Act (CCRA), CAL. CIV. CODE § 1798.82(a). (¶ 297.) Inmediata argues that Plaintiffs allege no facts demonstrating unreasonable delay in notifying them of the alleged breach, and therefore, Plaintiffs fail to state a CCRA violation. (Doc. No. 17-1 at 28.) Inmediata further argues that Plaintiffs did not allege harm or subsequent incremental harm from the delay. (*Id.*)

The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . . in the most expedient time possible and without unreasonable delay[.]" CAL. CIV. CODE § 1798.82(a).

Inmediata cites no authority to support its argument that 81 days is reasonable delay. Additionally, the only authority Inmediata cites to support its argument that Plaintiffs are required to allege harm or incremental harm from the delay is *Yahoo*, 2017 WL 3727318, at *41. In *Yahoo*, however, the court found the plaintiffs adequately alleged incremental harm by alleging that, if they had been notified earlier, they could have taken steps to mitigate the "fallout" from their information being stolen. *Id.* Similarly, Plaintiffs allege that because of the delay they were "prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze." (¶ 301.) Plaintiffs also allege these measures could have prevented some of their damages because their information would have been less valuable to identity thieves. (*Id.*) Although only one Plaintiff, Mr. White, allegedly experienced "fallout" in the form of identity theft, Inmediata does not specifically address Plaintiffs' allegations regarding their incremental harm. Instead, Inmediata argues, inaccurately, that "Plaintiffs here have not alleged harm

or subsequent 'incremental harm' from delay." (Doc. No. 17-1 at 28.) Accordingly, at this early stage in the litigation, Plaintiffs allege a plausible claim based on violations of the CCRA, and Inmediata has not met its burden of showing otherwise.

7. Minnesota Health Records Act

Plaintiffs allege that Inmediata violated the Minnesota Health Records Act (MHRA), MINN. STAT. ANN. §§ 144.29-144.34, by releasing their health records without first obtaining consent or authorization, and by negligently or intentionally releasing their health records. (¶¶ 312-13.) Inmediata argues these allegations are conclusory and not supported by factual allegations. (Doc. No. 17-1 at 28-29.) Inmediata also argues this claim should be dismissed because "Plaintiffs did not and cannot allege facts suggesting that any unauthorized person actually searched for, found, viewed, or downloaded the data at issue." (*Id.* at 29.) As discussed above, however, Plaintiffs allege that Inmediata posted their medical information on the internet for an unknown period of time. Additionally, Plaintiffs repeatedly allege that their information was viewed. Inmediata also provides no support for its argument that by posting medical information on the internet, where it was allegedly viewed, is insufficient to plead a plausible claim under the MHRA. Accordingly, at this early stage in the litigation, Plaintiffs allege a plausible claim based on violations of the MHRA, and Inmediata has not met its burden of showing otherwise.

8. Article I, Section 1 of the California Constitution

Finally, Inmediata argues that Plaintiffs' claim under the California Constitution it was not Inmediata.[23] (Doc. No. 17-1 at 29-30.) The California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. I, § 1. The

[23] Although Plaintiffs allege both invasion of privacy and violation of the California Constitution, (¶ 319), Inmediata does not move to dismiss Plaintiffs' invasion of privacy claim.

parties do not dispute that to support a claim under this provision, Plaintiffs must show: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 39-40 (1994). The parties also do not dispute that Plaintiffs have a legally protected privacy interest in their medical information. *See also Heldt v. Guardian Life Ins. Co. of Am.*, Case No. 16-cv-885-BAS-NLS, 2019 WL 651503, at *4 (S.D. Cal. Feb. 15, 2019) (recognizing a legally protected privacy interest in medical information held by an insurer).

Whether Plaintiffs had a reasonable expectation of privacy, and whether Inmediata's conduct constitutes a serious invasion of privacy, are mixed questions of law and fact. *See Hill*, 7 Cal. 4th at 40; *see also Facebook Tracking*, 956 F.3d at 606 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."). At this stage in the litigation, it is reasonable to infer that Plaintiffs reasonably expected Inmediata would not post their medical information on the internet, negligently or otherwise, and that doing so constitutes a serious invasion of privacy. Although some courts have dismissed privacy claims based on the state constitution given the "high bar" for such claims, *see Low*, 900 F. Supp. 2d at 1025 (listing cases), these cases do not involve medical information that was "posted" on the internet, *see Hill*, 7 Cal. 4th at 35 ("Legally recognized privacy interests [include] interests in precluding the dissemination or misuse of sensitive and confidential information."); *Strawn v. Morris, Polich & Purdy, LLP*, 30 Cal. App. 5th 1087, 1100 (2019) (finding the seriousness of the alleged invasion of privacy based on disclosure of plaintiffs' tax returns presented a question of fact that could not be resolved on demurrer). Moreover, Inmediata provides no support for its argument that negligently posting medical information on the internet does not constitute a serious invasion of privacy, and only those who hack or steal information can be held liable. *See Doe v. Beard*, 63 F. Supp. 3d 1159, 1170 (C.D. Cal. 2014) (negligent disclosure of plaintiff's medical information was sufficient to sustain a breach of privacy claim under the state constitution); *but see Razuki*

v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (suggesting the conduct must be intentional). Accordingly, at this early stage in litigation, Plaintiffs allege a plausible violation of the state constitution's privacy provision, and Inmediata has not met its burden of showing otherwise.

IV. CONCLUSION

For the foregoing reasons, Inmediata's Motion to Dismiss under Rule 12(b)(1) for lack of standing is **DENIED**. Inmediata's Motion to Dismiss under Rule 12(b)(6) is **DENIED IN PART** and **GRANTED IN PART**. Inmediata's Motion to Dismiss Plaintiffs' claims for negligence, breach of contract, violation of sections 56.101(a) and 56.36(b) of CMIA, as well as violations of the CCPA, CCRA, MHRA, and the California Constitution, is **DENIED**. Inmediata's Motion to Dismiss Plaintiffs' claims for unjust enrichment and violation of section 56.10(a) of CMIA is **GRANTED**. In their opposition to the instant motion, Plaintiffs do not request leave to amend. Inmediata's answer to the operative complaint is due ***within 21 days*** of this court's order.

IT IS SO ORDERED.

DATED: November 19, 2020

JEFFREY T. MILLER
United States District Judge