UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

CHANDRA TATE, *et al.*,

Plaintiffs, **Case Nos. 1:21-cv-36**

v.

JUDGE DOUGLAS R. COLE

EYEMED VISION CARE, LLC,

Defendant.

OPINION AND ORDER

Plaintiffs Chandra Tate, Barbara Whittom, and Alexus Wynn bring this putative class action lawsuit alleging that defendant EyeMed Vision Care, LLC (EyeMed) negligently maintained lax security protocols and failed to protect Plaintiffs' personally identifiable information (PII) from cybertheft. (Am. Compl., Doc. 19, ¶¶ 1–3, #221–22). As a result of this purported lax security, Plaintiffs alleged cybercriminals hacked an EyeMed email account and obtained the PII of EyeMed members (including Plaintiffs'), thereby increasing the likelihood of identity theft and financial fraud. (*Id.* at ¶¶ 3, 15, #222, #224). Plaintiffs seek class certification and damages[1] for their tort, contract, and state law claims. (*Id.* at #252–70). Defendant EyeMed now moves to dismiss arguing that Plaintiffs lack standing because they fail to assert a cognizable injury in fact traceable to either the data breach or EyeMed's

[1] Plaintiffs also request "declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other Class members." (Doc. 19, #270). But beyond this boilerplate language, Plaintiffs do not explain anywhere in the Complaint how forward-looking equitable relief should be fashioned. The Court will therefore construe their Complaint as a complaint for damages—the true heart of their claim.

actions and that Plaintiffs fail to allege a plausible claim for relief. (Doc. 21). The Court finds that Plaintiffs have standing and allege facts that plausibly support at least some of their claims. The Court therefore **GRANTS IN PART** and **DENIES IN PART** EyeMed's Motion to Dismiss (Doc. 21).

BACKGROUND

EyeMed is one of the largest vision benefits companies in the country, boasting over 60 million benefit members. (Doc. 19, ¶ 2, #222). EyeMed is organized in Delaware and maintains its principal place of business in Ohio. (*Id.* at ¶ 24, #227). As part of its business, EyeMed collects members' PII including their names, emails, addresses, health savings account information, and medical history. (*Id.* at ¶ 29, #228). If a member uses health insurance to obtain benefits, EyeMed also, through those insurance plans, collects that member's birthday and social security number. (*Id.* at ¶ 31, #228).

According to Plaintiffs,[2] EyeMed failed to take basic security measures to protect its members' data, such as adequate personnel training and routine system testing. (*Id.* at ¶ 44, #231). This failure is perhaps best exemplified by EyeMed's delayed response to the data breach that sparked this lawsuit.

On June 24, 2020, cybercriminals hacked an EyeMed email account and sent numerous phishing emails to addressees in the account's address book. (*Id.* at ¶ 48, #232). While it is unknown what information the cybercriminals accessed from the

[2] For purposes of this motion to dismiss, the Court accepts as true all of Plaintiffs' well-pleaded factual allegations. *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1311 (N.D. Ga. 2019).

account, a subsequent investigation revealed that emails in the hacked email account contained the names, contact information, dates of birth, vision insurance account numbers, and, for some members, the Social Security numbers of several EyeMed members. (*Id.* at ¶ 46, #231). EyeMed did not discover the data breach for a full week. (*Id.* at ¶ 48, #232). After EyeMed discovered the breach on July 1, 2020, it conducted its own investigation of the account to determine what information may have been compromised. (*Id.*).

But allegedly EyeMed was not entirely forthcoming either as to its discovery of the data breach or the results of its subsequent investigation. EyeMed did not disclose the security breach to anyone until September 28, 2020. (*Id.* at ¶ 47, #231–32). Even then, it disclosed the breach only to its insurance company affiliates. (*Id.*). Not until December 7, 2020, did EyeMed mail a notice to its members that alerted them that their personal data was exposed. (*Id.* at ¶ 48, #232). In the notice, EyeMed offered to provide no-cost identity monitoring services to all compromised members. (*See, e.g.*, Doc. 19–1, #275–76).[3]

A. Plaintiff Tate

Plaintiff Tate, a South Carolina resident, used EyeMed for her vision benefits from 2016–2019. (Doc. 19, ¶ 54, #233). Along with many other EyeMed members, Tate received a notice from EyeMed that her information was exposed in the June 24 data breach. (*Id.* at ¶ 56, #234). The notice stated that Tate's name, address, date of

[3] EyeMed used the name "Chandra Price" in the notice letter it sent to Plaintiff Tate as that was Plaintiff Tate's name at the time. She has since married. (Doc. 1, #5).

birth, phone number, email address, and vision insurance account number might have been accessed. (*Id.*). Before the data breach, Tate maintained her own credit monitoring policy, for around $53 a month. (*Id.* at ¶ 57, #234). Tate alleges that she planned to cancel the policy to reduce her monthly expenses but delayed doing so after the data breach. (*Id.*). She also began reviewing her credit reports, financial statements, and medical records for any indications of fraud. (*Id.*). Tate estimates that she spends about an hour a day monitoring her bank statements and credit card accounts for irregularities. (*Id.*).

After the data breach, Tate also received notice that her private information was found on the dark web. (*Id.* at ¶ 59, #235). In addition, she claims she began receiving a significantly increased number of suspicious and unsolicited telephone calls, text messages, and email messages. (*Id.*). She has received scam calls nearly every day since the data breach. (*Id.*). She spends around 12 hours per month responding to incidents related to the data breach and claims she now experiences emotional distress stemming from her fear of identity theft and fraud. (*Id.* at ¶¶ 60–61, #235).

B. Plaintiff Whittom

Plaintiff Whittom, a California resident, used EyeMed for her vision benefits from 2012–2015 and reupped her membership in 2019. (*Id.* at ¶ 63, #236). She received a notice from EyeMed that her name, address, and birthdate were compromised in the data breach. (*Id.* at ¶ 65, #236). Unlike the other plaintiffs, Whittom's Social Security number and health insurance ID number were also

allegedly exposed. (*Id.*). When EyeMed offered free credit monitoring, Whittom enrolled. (*Id.* at ¶ 66, #236–37). Since the data breach, Whittom has spent about 30 hours monitoring her bank statements and financial accounts for fraud. (*Id.*).

Whittom claims that, after the data breach, she received a significantly increased amount of scam and phishing calls, texts, and emails. (*Id.* at ¶ 68, #237). She says she receives such calls daily. (*Id.*). She also alleges that she has suffered emotional distress stemming from anxiety and fear of identity theft and fraud. (*Id.* at ¶ 70, #237–38).

C. Plaintiff Wynn

Plaintiff Wynn, a South Carolina resident, utilized EyeMed for vision benefits from 2016–2019. (*Id.* at ¶ 73, #238). She received a notice from EyeMed that her name, address, birthdate, phone number, email address, and vision insurance account number were allegedly exposed in the data breach. (*Id.* at ¶ 75, #239). Wynn, like Tate (who happens to be Wynn's mother), used credit monitoring services before the breach and maintained those services afterward. (*Id.* at ¶ 76, #239). Since the breach, Wynn has spent about 35 hours reviewing bank statements and financial accounts for fraud. (*Id.*).

After the data breach, Wynn discovered fraudulent charges on her credit card, which prevented her from using the credit card benefits program. (*Id.* at ¶ 78, #239–40). The inaccessibility of the credit card benefits program required her to borrow money from relatives for college tuition. (*Id.*). In a separate incident, Wynn received a letter from the IRS notifying her the IRS was withholding her 2020 tax refund until

it could properly identify Wynn. (*Id.*). The IRS cited potential fraud as the reason for the withholding. (*Id.*). On top of these fraud incidents, Wynn also received a significantly increased number of scam and phishing calls, texts, and emails. (*Id.*). Wynn claims she has suffered emotional distress stemming from fear of identity theft and fraud. (*Id.* at ¶ 80, #240).

D. The Plaintiffs' Claims

Based on these allegations, Plaintiffs bring tort, contract, and California state law claims (on behalf of the California plaintiff), alleging that EyeMed's failure to protect Plaintiffs' PII damaged them. Specifically, Plaintiffs allege: (1) EyeMed was negligent in maintaining their PII under both a traditional and negligence per se theory (Claims 1-2); (2) EyeMed breached an implied contract with Plaintiffs to adequately protect their PII (Claim 3); (3) EyeMed was unjustly enriched by Plaintiffs' membership premiums because it failed to protect their PII (Claim 4); and (4) and EyeMed violated several California consumer protection and medical regulation statutes (Claims 5-7). (*See generally* Doc. 19).

E. EyeMed's Motion to Dismiss

EyeMed has now moved to dismiss the action. Its arguments fall into two categories. First, it claims Plaintiffs lack standing, which, if true, means the Court lacks jurisdiction. On this front, EyeMed presses two primary arguments: (1) Plaintiffs' injuries (such as their fear of future identity theft, the increase in scam calls, and their alleged emotional distress) are too speculative or abstract to satisfy Article III's standing requirements, and (2) Plaintiffs' injuries are not traceable to the

data breach because the type of data exposed (names, phone numbers, and non-sensitive PII) could not plausibly cause identity theft or any other injury. Second, EyeMed says that even if Plaintiffs have standing, they have failed to allege any plausible claim for relief. Here, EyeMed says that any injuries Plaintiffs alleged (whether in contract or in tort) were not caused by the data breach because none of Plaintiffs injuries could have been caused by the release of non-sensitive PII. As to the California state law claims, EyeMed posits that the statutes are inapplicable.

LAW AND ANALYSIS

This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), (5), because the parties are at least minimally diverse,[4] the putative class exceeds 100 members, and the amount in controversy purportedly exceeds $5,000,000. Venue is proper because a substantial part of the events giving rise to the claims occurred in this district (EyeMed's headquarters are in Mason, Ohio). 28 U.S.C. § 1391(b)(2).

To survive a motion to dismiss under Fed. R. Civ. P. 12(b)(1) or 12(b)(6), Plaintiffs must allege "sufficient factual matter … to state a claim to relief that is

[4] Minimal diversity requires that at least one plaintiff is diverse from at least one defendant. *Life of the S. Ins. Co. v. Carzell*, 851 F.3d 1341, 1344 (11th Cir. 2017) (citing 28 U.S.C. § 1332(d)(2)(A)). Plaintiffs are citizens of South Carolina and California. The Complaint alleges that EyeMed LLC is a wholly owned subsidiary of Luxottica of America, Inc., which has its principal place of business in Mason, Ohio. (Doc. 19, ¶ 24, #227). Because the Complaint did not specify Luxottica's place of incorporation nor whether EyeMed had any other members, the Court ordered EyeMed to file a Citizenship Disclosure, which EyeMed did on September 29, 2023. That disclosure states that EyeMed is a single member LLC and that it is a citizen of Ohio. (Doc. 39). Considering the two together, the Court is satisfied that Luxottica is EyeMed's only member and that it is a citizen of Ohio, which in turn means EyeMed is a citizen of Ohio. Minimal diversity is therefore met in this case.

plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (cleaned up); *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021) ("A plaintiff must demonstrate standing with the manner and degree of evidence required at the successive stages of the litigation." (cleaned up)). While a "plausible" claim for relief does not require a showing of *probable* liability, it requires more than "a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (citation omitted). The complaint must allege sufficient facts that allows the Court to "draw the reasonable inference that the defendant is liable." *Id.*

At the motion-to-dismiss stage, the Court accepts the facts of the Complaint as true. *Id.* But that does not mean the Court must take everything Plaintiffs allege as gospel, no matter how far-fetched. The Court may disregard "naked assertions" of fact or "formulaic recitations of the elements of a cause of action." *Id.* (cleaned up).

As noted, Plaintiffs have asserted tort, contract, and California state law claims (on behalf of the California plaintiff), based on their allegations that EyeMed's failure to protect Plaintiffs' PII harmed them. EyeMed moves to dismiss the entire Complaint arguing that Plaintiffs lack standing and fail to state a claim for relief.

A. Standing

Article III § 2 of the Constitution limits a federal court's jurisdiction to "cases" and "controversies." A plaintiff's standing to sue is one element of this constitutional requirement. *TransUnion*, 141 S. Ct. at 2203. To demonstrate standing, a plaintiff must show: (1) that she suffered a concrete, particularized, and actual or imminent injury; (2) that the injury is traceable to the defendant's conduct; and (3) that a

favorable ruling would redress that injury. *Id.* An injury is "concrete," and therefore cognizable under Article III, when the type of injury bears a "close relationship" to a harm traditionally recognized at common law. *Id.* at 2204.

A future injury satisfies Article III only when it is "certainly impending" or there is a "substantial risk" that it will occur. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409, 414 n.5 (2013); *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). Anything lower, even an "objectively reasonable likelihood" of such harm, is insufficient. *Clapper*, 568 U.S. at 410.[5] And when a party takes costly steps to mitigate the risk of future harm, those costs do not create standing where the future harm is not "certainly impending." *Id.* at 416. Lastly, "standing is not dispensed in gross." *TransUnion*, 141 S. Ct. at 2208. As a result, every plaintiff must demonstrate standing for each claim and form of relief. *Id.*

Plaintiffs allege several theories of injury—almost all are inadequate to confer standing. To start, precedent forecloses many of them. For example, alleged injuries arising from the risk of future identity theft,[6] or the time spent monitoring financial

---

[5] The Supreme Court's precedent is unclear as to what work the "substantial risk" standard performs apart from the "certainly imminent" standard for future injury. As a matter of etymology, proving an injury is "certainly imminent" seems like a heavier burden. But then again the Court's holding in *Clapper* implies the "substantial risk" standard is more burdensome than it may first appear. According to the *Clapper* Court, proof of an "objectively reasonable likelihood" was *insufficient* to confer standing, but proof of a "substantial risk" of that same harm *would* be sufficient to confer standing. 568 U.S. at 410, 414 n.5. So whatever "substantial" means, it appears it is something well in excess of "likely."

[6] *See Clapper*, 568 U.S. at 410–15 (requiring a future injury to be "certainly impending"); *see also TransUnion*, 141 S. Ct. at 2210–11 (stating that risk of future harm rarely creates standing to sue for damages, unlike injunctive relief).

Wynn, unlike the other plaintiffs, has actually suffered from financial fraud since the data breach. (Doc. 19, ¶ 78, #239–40). But as EyeMed points out, none of Wynn's data maintained

accounts,[7] or emotional distress,[8] or an intangible violation of privacy,[9] all rely on arguments the Supreme Court has rejected.

Many of Plaintiffs' alternative novel theories of injury are implausible. Plaintiffs allege that their PII has intrinsic economic value, as shown by the booming corporate and black market for PII. (Doc. 19, ¶¶ 86–87, #242; Opp'n, Doc. 23, #357). They then allege that because their PII has a quantifiable market value and because cybercriminals allegedly stole their PII due to EyeMed's negligence, that this purported theft of personal property is itself an injury to Plaintiffs because it prevents Plaintiffs from capitalizing on the value of their PII. (Doc. 19, ¶ 87, #242; Doc. 23, #357–59). But Plaintiffs do not explain how they are injured by this. While businesses place a premium on the PII of potential customers for marketing purposes, individuals do not ordinarily reap financial gain from selling their information as a commodity. *Huynh v. Quora, Inc.*, No. 18-cv-7597, 2019 WL 11502875, at *7 (N.D. Cal. Dec. 19, 2019) ("Even if Quora may have gained money through its sharing or use of the Plaintiffs' information, that's different from saying the Plaintiffs lost money."

---

by EyeMed and exposed in the data breach could, alone, be used to commit financial fraud. (Doc. 21-1, #319).

[7] *See Clapper*, 568 U.S. at 416 (holding that mitigation measures cannot support standing without a certainly impending harm).

[8] *See Consol. Rail Corp. v. Gottshall*, 512 U.S. 532, 546–49 (1994) (describing the various common law tests for negligent infliction of emotional distress—none of which allowed for recovery based on pure emotional distress without an attendant physical impact or risk of physical harm).

[9] *See TransUnion* 141 S. Ct. at 2210 (requiring defendant's publication of defamatory material to assert defamation-based injury); *see also Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1240 (11th Cir. 2022) (en banc) (requiring evidence of publication to assert an injury based on a public disclosure tort analogue in a case dealing with a procedural violation under statute).

(cleaned up)). And even if such a sale were possible, Plaintiffs do not allege that they planned to make such a sale in the future. True, collecting PII is sometimes part of the exchange an individual makes when signing up for a service (e.g., Facebook captures various PII from its users that it then monetizes), and in that sense it has a "value" to its owner (as the service provider is willing to exchange the service for the PII). But Plaintiffs have not alleged that the theft of their PII from one entity will interfere with their ability to conduct such exchanges down the road (e.g., Facebook will not deny them an account because their PII has been stolen and is thus less valuable than it otherwise might be).

Nor does it appear to the Court that Plaintiffs could claim harm based on interference with their "ownership" interest in their PII, akin to conversion or trespass to chattels. To start, Plaintiffs have not pointed the Court to any law, and the Court is not aware of any, that creates property rights in PII.[10] And, even if such law exists, Plaintiffs have not explained *how* the value of their PII was diminished in the data breach, beyond presumptively claiming that it must have been. (Doc. 19, ¶¶ 15, 18, 102, #224–25, 248).

In short, Plaintiffs fail to allege facts which plausibly support this theory of injury.

---

[10] For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) does not fit the bill. HIPAA is a regulatory statute, imposing obligations on medical providers and mandating certain procedures for the protection of medical information. *Acara v. Banks*, 470 F.3d 569, 571 (5th Cir. 2006). It does not explicitly confer a property interest in a patient's medical information and courts would be hard pressed to find an implicit property interest given the consensus of authority stating that HIPAA does not create a private right of action. *Id.* at 572; *Dodd v. Jones*, 623 F.3d 563, 569 (8th Cir. 2010); *Mayfield v. Presbyterian Hosp. Admin.*, 772 F. App'x 680, 686 (10th Cir. 2019).

Plaintiffs also argue that money paid to EyeMed for vision benefits qualifies as an injury because "the monies or fees paid … were supposed to be used by EyeMed, in part, to pay for the administrative and other costs of providing reasonable data security." (Doc. 19, ¶ 161, #261). Plaintiffs' retroactive attempt to characterize consideration for vision benefits as payment for data security is a stretch to say the least. Plaintiffs do not allege that data security ever formed part of the contractual bargain for vision benefits. While Plaintiffs do allege they would not have used EyeMed if they had known of EyeMed's lax security protocols (*Id.* at ¶¶ 55, 64, 74, #234, 236, 238), those allegations in no way show that *EyeMed* contemplated data security as part of its commercial bargain. And of course, a meeting of the minds, at least as to essential terms, is a prerequisite to a binding contract—express or implied. *E.g.*, *Tocci v. Antioch Univ.*, 967 F. Supp. 2d 1176, 1195 (S.D. Ohio 2013). Because Plaintiffs fail to allege facts showing that data security was a condition of any bargain made between themselves and EyeMed—other than conclusory assertions to this effect, (Doc. 19, ¶ 155, #260)—this theory of injury is also unavailing.

But, while most of Plaintiffs' theories lack force, they do manage to find at least one needle in the standing haystack. Specifically, Plaintiffs claim that, after the data breach, they received a significantly increased number of scam and phishing calls, texts, and emails. (*Id.* at ¶¶ 59, 68, 78, #235, 237, 240). Such communications annoy, harass, and, in the case of phone calls, temporarily claim control over an individual's personal device. The Sixth Circuit has held that such unsolicited calls and messages constitute cognizable Article III injuries in fact. *See Dickson v. Direct Energy, LP*, 69

F.4th 338, 345 (6th Cir. 2023) (likening unsolicited calls and messages to the common law tort of intrusion-upon-seclusion). So Plaintiffs adequately allege a concrete and particularized injury—if barely.

Of course, beyond injury, they must also allege causation. In other words, they must plausibly tie the claimed harm to the challenged conduct. On that score, Plaintiffs allege that such calls significantly increased directly after the data breach. (Doc. 19, ¶¶ 59, 68, 78, #235, 237, 240). While Plaintiffs do not explicitly allege that the data breach "caused" that increased call volume, their point is clear—the increase is traceable to the data breach. *Parsons v. U.S. Dep't of Justice*, 801 F.3d 701, 715 (6th Cir. 2015). This allegation is plausible given the nature of the incident. EyeMed's email account was hacked by cybercriminals—individuals who presumably sought to profit from the cyberattack. (Doc. 19, ¶ 46, #231). And Plaintiffs allege that their names and addresses were compromised in addition to Tate's and Wynn's phone numbers. (*Id.* at ¶¶ 46, 56, 65, #231, 234, 236). Those allegations, coupled with the notification that Tate's contact information was found on the dark web, (*id.* at ¶ 59, #235), which is at least plausibly an information source for scam callers, create a "reasonable inference" that the data breach led to the increased number of scam calls. *Iqbal*, 556 U.S. at 678. Plaintiffs' injury is therefore sufficiently traceable to the data breach—and, by extension, EyeMed's conduct—for motion to dismiss purposes.

Lastly, a favorable ruling by this Court would redress Plaintiffs' injuries. Though hard to quantify, Plaintiffs' injuries sound in tort, and, like most traditional tort injuries, can be redressed by money damages.

EyeMed disagrees. It claims that the increase in scam calls is not traceable to the data breach and that Plaintiffs' allegations rest on the logically erroneous assumption (sometimes labeled post hoc ergo propter hoc) that anything occurring after an event necessarily must have resulted from that event. (Doc. 21-1, #320; Reply, Doc. 24, #385–86). While EyeMed correctly identifies this logical fallacy, it nonetheless ignores the commonsense principles and lax evidentiary standard that apply at the motion-to-dismiss stage. Plaintiffs need not *prove* that the data breach caused the increase in scam calls. They need only plausibly allege that that is the case. And because it is more than a "sheer possibility" that a data breach involving contact information would lead to an increased number of scam calls (indeed, Tate confirmed her information was on the dark web), Plaintiffs have adequately shown for present purposes that their injury is traceable to EyeMed's conduct. *Iqbal*, 556 U.S. at 678.

The Court finds that Plaintiffs have standing to bring their claims and therefore proceeds to the merits.

B. Merits

Plaintiffs allege negligence, negligence per se, breach of implied contract, unjust enrichment, and California state law claims. Before the Court considers these claims, a brief choice-of-law analysis is in order. When considering cases arising under a court's diversity jurisdiction, federal courts apply the choice-of-law rules of the forum state—in this case, Ohio. *Muncie Power Prods., Inc. v. United Tech. Auto., Inc.*, 328 F.3d 870, 873 (6th Cir. 2003). For tort actions, Ohio choice-of-law follows the

Restatement of the Law of Conflicts, which turns on which state possesses the most significant relationship to the tort injury. *Morgan v. Biro Mfg. Co., Inc.*, 474 N.E.2d 286, 289 (Ohio 1984). Factors relevant to the significant relationship test include the place of injury, the residence of the parties, and the place where the relationship of the parties is centered. *Id.* For contract actions, the test is the same, where the factors bearing on the "most significant relationship" include the place of contracting and negotiation, the place of performance, the location of the subject matter, and the residence of the parties. *Ohayon v. Safeco Ins. Co. of Ill.*, 747 N.E.2d 206, 209 (Ohio 2001).

The Court finds based on the allegations in the Complaint that Ohio has the most significant relationship to this suit. EyeMed is headquartered in Ohio and presumably carries out its operations there. (Doc. 19, ¶ 24, #227). A data breach is difficult to "place" in any physical location because such events, by their nature, occur over computer networks with the various actors located wherever they may choose to be. So the place of injury factor provides little value. Plaintiffs allege that they entered into an implied contract with EyeMed to protect their PII. (*Id.* at ¶¶ 149–55). But Plaintiffs themselves label the purported contract "implied," meaning there was no place of explicit negotiation or acceptance, so this factor is similarly unhelpful. That leaves the residence of the parties. The named Plaintiffs are scattered across two states and seek to certify a nationwide class, which would presumedly increase that count significantly. The Court therefore finds the residence of the defendant determinative—at least for present purposes. The Court accordingly applies Ohio law

in assessing the plausibility of the tort and contract actions raised here. For the California state law claims, the Court will of course apply California law.

1. Negligence and Negligence Per Se

As every first-year law student learns, a plaintiff alleging negligence must show a duty the defendant owes to the plaintiff, a breach of that duty, and a resulting injury. *Rieger v. Giant Eagle, Inc.*, 128 N.E.3d 1121, 1125 (Ohio 2019). To demonstrate negligence per se, which is not a standalone claim but a theory of proof, a plaintiff must show that a defendant violated a statutorily defined standard of care and that the violation caused the plaintiff's injuries. *Sikora v. Wenzel*, 727 N.E.2d 1277, 1280 (Ohio 2000). Under a negligence per se theory, the statutory violation proves the breach element. *Id.*

Plaintiffs allege that EyeMed, by collecting and using Plaintiffs' PII in the course of its business, owed a duty of reasonable care to protect and to secure Plaintiffs' PII from the foreseeable harm of a data breach. (Doc. 19, ¶¶ 34–36, 118, #229, #252–53). They further allege that EyeMed breached this duty by failing to follow reasonable security standards, adequately train personnel, conduct routine system testing, and maintain adequate computer systems. (*Id.* at ¶¶ 44, 125, #231, #254–55). Lastly, Plaintiffs allege that EyeMed's failure proximately caused them the injuries they allege because (1) data breaches are foreseeable in the medical industry, and (2) so are the resulting injuries of the type claimed here. (*Id.* at ¶¶ 36, 128, #229, #255–56).

In its opposition, EyeMed does not address duty or breach, but instead places all its eggs in the injury and causation baskets. It argues that any injuries Plaintiffs sustained were not proximately caused by the data breach because the data breach did not expose sufficiently sensitive information to increase the risk of identity theft. (Doc. 21-1, #311–15, #324). But Plaintiffs' claimed injury stems from the significant increase in scam and phishing calls, not just the alleged identity theft. And EyeMed does not dispute that Plaintiffs' contact information was leaked in the breach—which is all that's required to initiate scam calls. While EyeMed does argue that the increase in scam calls is not traceable to the data breach, the Court rejects this argument for the same reasons that lead the Court to find that Plaintiffs have standing. That is to say, the allegations in the Complaint plausibly establish a causal nexus between the exposed PII and the resultant increase in scam calls: one reasonably follows from the other.

EyeMed next argues that Plaintiffs' claims fail because they allege only economic injuries which are not compensable in tort under the economic loss rule. (Doc. 21-1, #324–25). The Court is not persuaded. The economic loss rule bars recovery in tort for injuries sustained under a contract. *Chemtrol Adhesives, Inc. v. Am. Mfrs. Mut. Ins. Co.*, 537 N.E.2d 624, 630–31 (Ohio 1989). The dividing line between a contract-based economic loss and a tort-based compensable injury lies in the source of the defendant's duty. *Id.* at 630. If a contract imposes the duty, the loss is not compensable; if the common law, then the injury is compensable in tort. *Id.* at 630–31. Plaintiffs alleged that EyeMed owed a common law duty of reasonable care

to protect their PII from misappropriation. (Doc. 19, ¶ 119, #253). EyeMed did not dispute this point in its memorandum, so its economic loss argument falls flat.

Confined to the injury for which Plaintiffs have standing, *Price v. Medicaid Dir.*, 838 F.3d 739, 746 (6th Cir. 2016), the Court finds that Plaintiffs' negligence claim is plausible, which is the only question at this juncture, *Iqbal*, 556 U.S. at 678. They alleged that data breaches are foreseeable and therefore EyeMed owed a duty to take reasonable steps to prevent such breaches and the injuries flowing from them—citing data to support their argument. (Doc. 19, ¶ 36, #229) (noting that healthcare data breaches tripled from 2018 to 2019 and that 41 million patient records were compromised by data breaches in 2019 alone). They further alleged that EyeMed breached that duty by failing to implement commonsense security protocols, (*id.* at ¶ 43, #231)—an allegation that EyeMed does not dispute for motion to dismiss purposes. They finally claim that EyeMed caused their injury because of the foreseeable nexus among EyeMed's lax security, the data breach, and the increased scam calls, (*id.* at ¶¶ 3, 59, 68, 78, #222, 235, 237, 240)—allegations the Court credits for reasons it cited to support a finding that Plaintiffs have standing: the causal nexus between Plaintiffs' injury and EyeMed's conduct is plausibly supported by reasonable inferences drawn from the allegations in the Complaint.

Because the Court finds Plaintiffs' negligence claim plausible, it need not evaluate whether they can alternatively prove the very same claim via a negligence per se theory, which as noted above is not a separate, standalone claim.

2. Breach of Implied Contract

Under Ohio law, an implied contract[11] is a binding agreement based on mutual assent that, unlike an express contract, can be inferred from surrounding circumstances. *See Union Sav. Bank v. Lawyers Title Ins. Corp.*, 946 N.E.2d 835, 841 (Ohio Ct. App. 2010). An implied contract is still a contract requiring proof of a meeting of the minds; but the proof required may be shown by tacit understanding rather than an explicit offer and acceptance. *Id.*

Plaintiffs allege that they and EyeMed entered into an implied contract "under which EyeMed agreed to safeguard and protect" Plaintiffs' PII. (Doc. 19, ¶ 149, #259). Beyond this threadbare allegation, Plaintiffs fail to allege any facts to support the claim that EyeMed agreed to provide data security as a condition of service—even tacitly. Simply stating that an implied contract existed is insufficient. *Iqbal*, 556 U.S. at 678. Thus, the Court finds the breach of implied contract claim implausible on its face.

3. Unjust Enrichment

Under Ohio law, an unjust enrichment claim requires the plaintiff to prove: (1) that she conferred a benefit upon the defendant, (2) the defendant knew about the benefit, and (3) it would be unjust for the defendant to retain the benefit without payment. *Padula v. Wagner*, 37 N.E.3d 799, 813 (Ohio Ct. App. 2015).

[11] It is also sometimes called an implied-in-fact contract, which differs from an implied-in-law contract. Despite the name, an implied-in-law contract is not actually a contract at all, but rather a form of substantive restitution law, which is designed to prevent unjust enrichment. *Spectrum Benefit Options, Inc. v. Med. Mut. Of Ohio*, 880 N.E.2d 926, 934 (Ohio Ct. App. 2007).

Plaintiffs allege that they conferred a monetary benefit on EyeMed through payments for vision benefits. (Doc. 19, ¶ 160, #260). But a traditional exchange of payment for goods and services is not a circumstance in which it is "unjust" to allow the defendant to retain the benefit. Plaintiffs got what they paid for—vision benefits. *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1249 (D. Colo. 2018) ("Plaintiffs paid for burritos; Plaintiffs received burritos."). Because EyeMed was not unjustly enriched by Plaintiffs' vision benefits premiums, this claim is implausible on its face.

4. California State Law Claims

Plaintiff Whittom brings several California state law claims on behalf of herself and putatively on behalf of the entire California subclass.

a. California Unfair Competition Law

Whittom alleges that EyeMed violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq., which prohibits business practices that are "unlawful, unfair, or fraudulent." *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-cv-14, 2016 WL 6523428, at *11 (S.D. Cal. Nov. 3, 2016) (cleaned up). She details several ways EyeMed supposedly violated the law but none of them save her claim. (Doc. 19, ¶¶ 169–77, #262–65). California's unfair competition law imposes a heightened injury requirement for non-state actors bringing suit. *Dugas*, 2016 WL 6523428, at *11. On top of an Article III injury in fact, the statute requires plaintiffs to show they specifically suffered a deprivation of money or property as a prerequisite to suit. Cal. Bus. & Prof. Code § 17204.

Whittom fails to allege facts showing that she has lost money or property as a direct result[12] of the data breach. Her conclusory allegation that she has lost money or property, without any supporting facts, cannot survive a motion to dismiss. (Doc. 19, ¶ 175, #265). She alleges she has suffered various intangible injuries including loss of time[13] and risk of future harm, but these are not sufficient under the statute. *Dugas*, 2016 WL 6523428, at *11. Because she does not allege that she has lost money or property, Whittom fails to state a California Unfair Competition Law claim upon which relief can be granted.

b. California Confidentiality of Medical Information Act

Whittom alleges that EyeMed violated Cal. Civ. Code § 56.101 by failing to "maintain and preserve the confidentiality of [her] medical information." (Doc. 19,

[12] As already stated, Plaintiffs claim that monies paid for vision benefits should count as an injury supporting standing. While Whittom does not use this argument in support of her unfair competition claim in the Complaint, she raises it in response to EyeMed's motion to dismiss. (Doc. 23, #370–71). But for the reasons already stated, this unjust enrichment argument does not satisfy the heightened injury requirement—it is facially implausible that fees for vision benefits formed part of a fictitious bargain for data security.

[13] Whittom claims that "California courts have found [Unfair Competition Law] standing based on allegations of an increased risk of future harm coupled with a loss of time spent dealing with the fallout from a data breach," and cites three cases in support. (*See* Doc. 23, #372 (citing *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024 (N.D. Cal. 2019); *Huynh*, 2019 WL 11502875; *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-2617, 2016 WL 3029783 (N.D. Cal. May 27, 2016))). Her reliance on these cases is misleading at best. While the cases cited did find loss of time sufficient to confer *Article III standing*, none found loss of time sufficient to bring a claim under Cal. Bus. & Prof. Code § 17204. *See Bass*, 394 F. Supp. 3d at 1035, 1039–40; *Huynh*, 2019 WL 11502875, at *4–6; *In re Anthem*, 2016 WL 3029783, at *30 (differentiating Article III standing and "UCL Standing" but finding plaintiff showed both because of loss of money). In fact, in two of the cases cited the district court *dismissed* the unfair competition claim because the plaintiff failed to allege loss of money or property. *See Bass*, 394 F. Supp. 3d at 1040–41; *Huynh*, 2019 WL 11502875, at *6 (dismissing because decline in value of PII and failure to realize full benefit of bargain with service provider were not losses of money or property). Whittom's argument fails to save her claim.

¶¶ 182–83, #266). But as EyeMed points out, the California statute covers only *medical information*, which is defined as "any individually identifiable information … regarding a patient's medical history, mental health application information, mental or physical condition, or treatment." Cal. Civ. Code § 56.05. Whittom does not specifically allege that any of her medical information was compromised—only her personal and financial information.[14] (Doc. 19, ¶ 65, #236); *Eisenhower Med. Ctr. v. Sup. Ct.*, 172 Cal. Rptr. 3d 430, 434 (Cal. Ct. App. 2014) (distinguishing between "individually identifiable information" and "medical information"). Whittom's name, phone number, or Social Security number do not constitute "medical information" as the statute defines the term. She therefore fails to state a claim for relief under California's Confidentiality of Medical Information Act.

c. California Consumer Privacy Act

Lastly, Whittom alleges that EyeMed violated Cal. Civ. Code § 1798.100(e) by failing to implement reasonable security measures to protect its customers' personal information. (Doc. 19, ¶¶ 193–96, #268–69); *see also* Cal. Civ. Code § 1798.150(a). Once again, the statute does not cover EyeMed's conduct—this time because EyeMed is a covered entity subject to HIPAA. (*See* Doc. 19, ¶¶132–33, #256 (alleging that EyeMed is bound by HIPAA)); *see also* Cal. Civ. Code § 1798.145(c)(1)(A) (exempting entities covered by HIPAA).

[14] Once again, Whittom's blanket allegation that EyeMed negligently stored her medical information, without any supporting facts, fails *Iqbal's* pleading standard. 556 U.S. at 678.

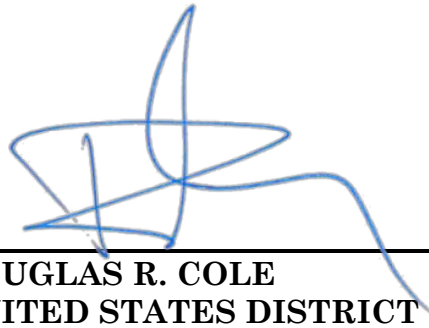
Whittom counters that § 1798.145(c) exempts the exposure of *medical information* covered by HIPAA from the California statute's coverage but that exposed *non-medical information* still can trigger liability under the law. (Doc. 23, #375 (citing *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020))). While it is true the *Stasi* court refused to dismiss a California Consumer Privacy Act claim based on this medical versus non-medical distinction,[15] this Court declines to follow *Stasi*'s lead. *Mid-Century Ins. Co. v. Fish*, 749 F. Supp. 2d 657, 667 (W.D. Mich. 2010) ("[A] federal court's interpretation of state law is not binding." (emphasis omitted)). *Stasi*'s analysis was perfunctory: it permitted the claim to go forward because the defendant had not addressed the non-medical information that was purportedly accessed. 501 F. Supp. 3d at 924. And *Stasi* failed to consider the fact that subparagraph (B) of § 1798.145(c)(1) exempts "*provider*[*s*]" of health care (who are subject to HIPAA) from the statute "to the extent the provider … maintains *patient information* in the same manner as medical information." (emphasis added). EyeMed cites the entirety of § 1798.145(c)(1) and asserts that it is exempt as a "covered entity." (Doc. 21-1, #328). Whittom does not challenge this and fails to provide specific allegations that EyeMed maintains non-medical patient information in a different manner than medical information—a fact required to establish the California statute covers EyeMed. Whittom therefore fails to state a claim for relief under California's Consumer Privacy Act.

[15] *Stasi* involved medical information covered by the California Confidentiality of Medical Information Act (CMIA) and did not mention HIPAA. 501 F. Supp. 3d at 924. But the consumer protection act exempts medical information covered by both CMIA and HIPAA and treats the two statutes identically, so the logic is the same. Cal. Civ. Code § 1798.145(c).

CONCLUSION

For the reasons stated, EyeMed's motion to dismiss (Doc. 21) is **GRANTED IN PART AND DENIED IN PART.** The motion is **DENIED** with respect to EyeMed's 12(b)(1) ground seeking to dismiss for lack of jurisdiction and **DENIED** with respect to EyeMed's 12(b)(6) ground seeking to dismiss Plaintiffs' negligence claim. The motion is **GRANTED** as to Plaintiffs' remaining claims, and the Court **DISMISSES** those claims, but **WITHOUT PREJUDICE**.

SO ORDERED.



September 29, 2023
DATE

DOUGLAS R. COLE
UNITED STATES DISTRICT JUDGE