UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

STEPHEN CAHILL, *et al.*, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	
v.	)	Case No. 1:23-cv-168
MEMORIAL HEART INSTITUTE, LLC, d/b/a The Chattanooga Heart Institute,	)	Judge Curtis L. Collier
Defendant.	)	

M E M O R A N D U M

Before the Court is Defendant's motion to dismiss Plaintiffs' consolidated complaint under Federal Rule of Civil Procedure 12(b)(6). (Doc. 27.) Plaintiffs responded in opposition. (Doc. 31.) The deadline for Defendant to file a reply was January 15, 2024. (Doc. 26.) On January 16, 2024, Defendant moved for a one-day extension of time to file a reply brief, stating that lead counsel had been unable to file due to illness. (Doc. 33.) Defendant filed a reply the same day. (Doc. 34.) For good cause shown, Defendant's motion for extension of time (Doc. 33) will be **GRANTED** to the extent Defendant's reply (Doc. 34) is considered timely.

Both parties supplemented their filings (Docs. 37, 39) and Plaintiffs responded to Defendant's supplemental filing (Doc. 38). For the reasons set out below, the Court will **GRANT in part** and **DENY in part** Defendant's motion to dismiss (Doc. 27).

I. BACKGROUND[1]

Defendant is a healthcare service provider headquartered in Chattanooga, Tennessee, with five locations in Tennessee and one in Georgia. (Doc. 24 ¶¶ 2, 82.) Plaintiffs are current and

[1] This summary of the facts accepts all the factual allegations in Plaintiffs' amended complaint as true, *see Gunasekera v. Irwin*, 551 F.3d 461, 466 (6th Cir. 2009).

former patients of Defendant whose private information was accessed in a data breach by third-party cybercriminals. (*Id.* ¶¶ 88, 91, 96–97, 164.) All named Plaintiffs live in either Tennessee or Georgia. (*Id.* ¶¶ 31, 38, 45, 52, 58, 64, 70.)

As part of its operations, Defendant "collects, maintains, and stores" personally identifiable information provided by current and former patients, including name, address, phone number, social security number, and clinical and financial information. (*Id.* ¶ 84.) "Defendant also creates and stores . . . other protected health information for its patients." (*Id.* ¶ 85.) Patients are provided Defendant's privacy policy, which represents that Defendant understands that patients' information must be protected. (*Id.* ¶ 86.)

On or before April 17, 2023, cyberthieves gained unauthorized access to Defendant's information technology network. (*Id.* ¶¶ 90–91, 98.) Through the cyberattack, the criminal third-parties accessed and exfiltrated private health and personal information (collectively "PII"), including social security numbers, of Plaintiffs and other current and former patients. (*Id.* ¶¶ 96–97.) Although Defendant discovered on May 31, 2023, that the cyberthieves had accessed 170,450 individuals' private information in the data breach, Defendant did not notify the individuals identified as affected until July 28, 2023. (*Id.* ¶¶ 91–92.) More than two months later, Defendant disclosed that 411,000 people had been affected by the data breach, most of which were first notified on October 6, 2023. (*Id.* ¶¶ 93–94.)

Since Defendant discovered the data breach, the cybercrime group "Karakurt" publicly claimed responsibility for the cyberattack. (*Id.* ¶ 98.) The "group exploits vulnerabilities or weak credentials of the computer network." (*Id.*) "Although Karakurt's primary extortion leverage is a promise to delete stolen data and keep the incident confidential, some victims reported Karakurt

actors did not maintain the confidentiality of victim information after a ransom was paid." (*Id.* ¶ 112.)

Cyberattacks and data breaches have become increasingly common, including against healthcare providers. (*Id.* ¶¶ 105–09.) Plaintiffs allege the risk of a cyberattack "was surely known to Defendant." (*Id.* ¶ 110.) Plaintiffs assert "on information and belief" the information accessed in the data breach was unencrypted. (*Id.* ¶ 99.) Plaintiffs also assert that if Defendant had "properly monitored its cyber security systems, it would have prevented the [d]ata [b]reach, discovered [it] sooner, and/or have prevented the hackers from accessing Plaintiffs' and [c]lass [m]embers' [PII]." (*Id.* ¶ 100.) Plaintiffs state that Defendant's failure to safeguard PII was "the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, [and] hacking attacks." (*Id.* ¶ 135.)

Plaintiffs assert "Defendant did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and [c]lass [m]embers." (*Id.* ¶ 123.) Plaintiffs list cybersecurity industry standards and best practices from multiple public and private sources and assert Defendant "could and should have implemented" the standards. (*Id.* ¶¶ 125–32.) According to Plaintiffs, the occurrence of the data breach indicates Defendant failed to implement at least one of the established cybersecurity measures. (*Id.* ¶ 133.)

Plaintiffs list acts or omissions by Defendant, which include "[f]ailing to adequately protect patients' [PII]," and "[f]ailing to test and assess the adequacy of its data security systems." (*Id.* ¶ 134.) According to Plaintiffs "Defendant failed to properly implement basic data security practices" set forth and published by the Federal Trade Commission ("FTC") and "did not use reasonable security procedures and practices . . . causing the exposure of [PII]." (*Id.* ¶¶ 113, 117.) Specifically, the FTC "recommends that companies not maintain [PII] longer than is needed for

authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures." (*Id*. ¶ 116.)

In response to the breach, Defendant offered one year of allegedly inadequate credit-monitoring services, for which Plaintiffs had to affirmatively sign up. (*Id*. ¶ 162.) Plaintiffs and proposed class members are at an increased and immediate risk of fraud and identity theft. (*Id*. ¶ 102, 136, 158.) They have incurred out-of-pocket expenses for protective measures such as credit monitoring fees and credit card freeze fees. (*Id*. ¶ 173.) Plaintiffs also lost the "value of their time" spent "to remedy or mitigate the effects of the [d]ata [b]reach," including identifying fraudulent loans and purchasing credit monitoring prevention tools. (*Id*.) Because there is often lag time between theft of information and its use, Plaintiffs must continue to monitor their financial information in the future. (*Id*. ¶¶ 155, 158–59.) They will continue to incur the costs of protective measures and "face substantial risk of out-of-pocket fraud losses." (*Id*. ¶¶ 165, 167.) More specifically, since the data breach Plaintiff Sidney Jackson experienced "identity theft and fraud, including a $14 fraudulent charge on her credit card." (*Id*. ¶ 48.) This required her to order a new credit card. (*Id*.) Also since the data breach, Plaintiff Elyn Painter has received what appear to be fraudulent calls and text messages which she believes are related to the data breach. (*Id*. ¶ 73.) She has spent time monitoring financial accounts and requesting a new debit card in response to the fraudulent communications. (*Id*. ¶ 75.) In a data breach "[e]arly notification helps a victim . . . mitigate their injuries, and . . . delayed notification causes more harm and increases the risk of identity theft." (*Id*. ¶ 174.)

Additionally, Plaintiffs "suffered a loss of value" of their PII. (*Id.* ¶ 168.) There is an "active and robust legitimate marketplace for PII." (*Id.* ¶ 169.) Consumers can sell non-public information to a data broker who "aggregates the information and provides it to markets or app[lication] developers." (*Id.*) One company pays consumers fifty dollars per year to people who agree to provide the company with their web browsing history. (*Id.*) Because Plaintiffs' PII was released without compensation, Plaintiffs lost both the "inherent market value" of the data as well as the loss of "the rarity of the [d]ata," which diminishes its market value. (*Id.* ¶ 170.)

Finally, Plaintiffs have "suffered a loss of privacy," and have anxiety that their PII may be disclosed more widely, which would further deprive them of privacy and cause embarrassment. (*Id.* ¶¶ 177–78.) All of the harm done to Plaintiffs was worsened by "Defendant's delay in identifying and reporting the [d]ata [b]reach." (*Id.* ¶ 174.) Plaintiffs' PII remains in Defendant's possession and Plaintiffs "have an interest in ensuring that their [PII] . . . is protected from future breaches." (*Id.* ¶ 176.)

This case is a consolidation of five separate actions against Defendant filed in August 2023. (Doc. 12 at 2.) The cases were consolidated on October 3, 2023, and the Court ordered Plaintiffs to file a consolidated complaint. (Doc. 20 at 2.) On November 2, 2023, Plaintiffs filed a consolidated complaint on behalf of themselves and a proposed nationwide class consisting of "[a]ll persons whose [PII] was actually or potentially accessed or acquired during the [d]ata [b]reach for which Defendant provided [n]otice of the [d]ata [b]reach beginning on or around July 28, 2023," but excluding, among others, "Defendant's officers, directors, and employees." (Doc. 24 ¶¶ 180–81.) Plaintiffs assert claims for (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) unjust enrichment; (5) bailment; (6) breach of fiduciary duty; (7) invasion of

privacy; and (8) declaratory and injunctive relief. Defendants moved to dismiss the complaint on December 14, 2023. (Doc. 27.) This matter is now ripe for review.

II. STANDARD OF REVIEW

A defendant may move to dismiss a claim for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). In ruling on a motion to dismiss under Rule 12(b)(6), a court must accept all the factual allegations in the complaint as true and construe the complaint in the light most favorable to the plaintiff. *Gunasekera v. Irwin*, 551 F.3d 461, 466 (6th Cir. 2009) (quotation and citation omitted). "[A]llegations asserted upon information and belief are not *per se* insufficient to withstand a Rule12(b)(6) motion; the Court must consider the pleading's factual allegations as a whole. *Glob. Licensing, Inc. v. Namefind Ltd. Liab. Co*., 582 F. Supp. 3d 467, 479 (E.D. Mich. 2022) (*citing Smith v. Gen. Motors LLC*, 988 F.3d 873, 885 (6th Cir. 2021) ("complaints grounding claims on 'information and belief' can survive a motion to dismiss" if they "set forth a factual basis for such belief"); *Gold Crest, LLC v. Project Light, LLC*, 525 F. Supp. 3d 826, 837 n.10 (N.D. Ohio 2021) ("Factual allegations based upon information and belief may be sufficient to support a plausible claim for purposes of Rule 12(b)(6) analysis where the factual allegations in the entire pleading allow the Court to draw the reasonable inference that defendant is liable for the conduct alleged.") (citation omitted) (emphasis in original). The court is not, however, bound to accept bare assertions of legal conclusions as true. *Papasan v. Allain*, 478 U.S. 265, 286 (1986); *see 16630 Southfield Ltd. P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502, 506 (6th Cir. 2013). "'[N]aked assertions devoid of further factual enhancement' contribute nothing to the sufficiency of the complaint." *Flagstar Bank*, 727 F.3d at 506 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

In deciding a motion under Rule 12(b)(6), a court must determine whether the complaint contains "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Although a complaint need only contain a "short and plain statement of the claim showing that the pleader is entitled to relief," *Iqbal*, 556 U.S. at 677–78 (quoting Fed. R. Civ. P. 8(a)(2)), this statement must nevertheless contain "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678.

Plausibility "is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (quoting *Twombly*, 550 U.S. at 556). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief.'" *Id.* at 679 (quoting Fed. R. Civ. P. 8(a)(2)) (alteration in original). "The factual allegations in the complaint need to be sufficient to give notice to the defendant as to what claims are alleged, and the plaintiff must plead 'sufficient factual matter' to render the legal claim plausible, i.e., more than merely possible." *Prows v. City of Oxford*, No. 1:22-cv-693, 2023 U.S. Dist. LEXIS 100018, at *7 (S.D. Ohio June 7, 2023) (quoting *Fritz v. Charter Twp. of Comstock*, 592 F.3d 718, 722 (6th Cir. 2010) (citing *Iqbal*, 556 U.S. at 678 (2009))). In determining whether the complaint satisfies facial probability, a court must "draw on its judicial experience and common sense." *See Iqbal*, 556 U.S. at 679.

If a party presents matters outside the pleadings in connection with a motion to dismiss, the court must either exclude those matters from consideration or treat the motion as one for summary judgment. Fed. R. Civ. P. 12(d).

III. DISCUSSION

Plaintiffs plead eight counts against Defendant: (1) negligence; (2) negligence per se; (3) breach of implied contract; (4) unjust enrichment; (5) bailment; (6) breach of fiduciary duty; (7) invasion of privacy; and (8) declaratory and injunctive relief.

A. Choice of Law

Preliminarily, the Court must determine which state's law applies to Plaintiffs' claims. This Court has jurisdiction under the Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119 Stat. 4 (2005) ("CAFA"). CAFA confers federal jurisdiction over certain class actions where: (1) the proposed class contains at least 100 members; (2) minimal diversity exists between the parties; and (3) the aggregate amount in controversy exceeds $5,000,000. 28 U.S.C. § 1332(d). The consolidated complaint alleges that there are over one hundred class members and the aggregate amount of the class members' claims exceed five million dollars. Additionally, Defendant is headquartered in Tennessee, while at least one Plaintiff at least one member of the class is a citizen of a different state than Defendant.

"A federal court sitting in diversity ordinarily must follow the choice-of-law rules of the State in which it sits." *Atlantic Marine Const. Co v. U.S. Dist. Ct. for the W. Dist. of Tex.*, 571 U.S. 49, 65 (2013) (citation omitted). Tennessee applies the "most significant relationship test" to tort claims, which provides that the law of the state where the injury occurred applies unless some other state has a more significant relationship to the litigation. *See Hataway v. McKinley*, 830 S.W.2d 53, 59 (Tenn. 1992). To determine the state with the most significant relationship, courts must consider several factors: (1) the place where the injury occurred; (2) the place where the conduct causing the injury occurred; (3) the domicile, residence, nationality, place of incorporation, and place of business of the parties; and (4) the place where the relationship, if any,

between the parties is centered. *Id.* In contract cases, Tennessee law provides that a contract is governed by the law of the state where it was executed. *See Williams v. Smith*, 465 S.W.3d 150, 153 (Tenn. Ct. App. 2014) (citation omitted).

In this case, the court will apply Tennessee law to the tort claims because Tennessee is the state with the most significant relationship. *Id.* While the proposed class is nationwide, meaning that Plaintiffs' domiciles vary and that the alleged injuries occurred in different states, the remaining factors point to Tennessee being the state with the most significant relationship. The data breach appears to have occurred primarily in Tennessee, and Defendant, whose conduct is the common denominator among the proposed class, is based in Tennessee. The Court will therefore apply Tennessee law to the tort claims. For the contract claim, the Court will apply Tennessee law for the same reasons; although there is not a written contract, any contractual duties were bestowed on Tennessee-based businesses, and the alleged breach-of-implied-contract claim relies on actions taken in Tennessee.

B. Effect of Amended Tennessee Law on Plaintiffs' Claims

Defendant filed a supplemental memorandum (Doc. 37) arguing that Tennessee Code Annotated Section 29-34-215, enacted on May 21, 2024, bars Plaintiffs' class claims. (Doc. 37, at 3.) The Court will treat this argument as part of Defendant's Rule 12(b)(6) motion.

Section 29-34-215 provides in relevant part, "[a] private entity is not liable in a class action lawsuit resulting from a cybersecurity event unless the cybersecurity event was caused by willful and wanton misconduct or gross negligence on the part of the private entity." Tenn. Code Ann. § 29-34-215(1)(b). Section 2 of §29-34-215 states "[t]his act takes effect upon becoming a law." The statute does not expressly state that it applies retroactively. *See* Tenn. Code Ann. § 29-34-215.

Defendant contends that Section 29-34-215 applies retroactively and the consolidated complaint fails to allege "willful and wanton misconduct or gross negligence" with sufficient plausibility. (Doc. 37 at 4; Doc. 39 at 2.) The court recently considered a nearly identical issue in *Haney v. Charter Foods N., LLC*, No. 2:23-cv-46, 2024 U.S. Dist. LEXIS 159245 (E.D. Tenn. Aug. 28, 2024), and held that Section 29-34-215 does not apply retroactively.

"Generally, statutes are presumed to operate prospectively and not retroactively." *Kee v. Shelter Ins.*, 852 S.W.2d 226, 228 (Tenn. 1993) (citing *Woods v. TRW, Inc.*, 557 S.W.2d 274, 275 (Tenn. 1977); *Cates v. T.I.M.E., DC, Inc.*, 513 S.W.2d 508, 510 (Tenn. 1974)). "For a statute to overcome this presumption and apply to pending litigation, it must be 'remedial or procedural in nature.'" *Haney*, No. 2:23-cv-46, 2024 U.S. Dist. LEXIS 159245, at *22 (quoting *Kee*, 852 S.W.2d at 228). "A procedural or remedial statute is one that does not affect the vested rights or liabilities of the parties. A procedural statute is one that addresses the mode or proceeding by which a legal right is enforced." *In re D.A.H.*, 142 S.W.3d 267, 273 (Tenn. 2004) (quoting *Nutt v. Champion Int'l Corp.*, 980 S.W.2d 365, 368 (Tenn. 1998)).

In *Haney*, the court found Section 29-34-215 "is focused predominantly on substantive law related to cybersecurity; the reference to class actions . . . represents the extent of its procedural or remedial interests." No. 2:23-cv-46, 2024 U.S. Dist. LEXIS 159245, at *23 (citing Tenn. Code Ann. § 29-34-215) (emphasis removed). Section 29-34-215 "draws its distinction based on a defendant's substantive conduct"—willful and wanton misconduct or gross negligence—rather than baring class actions "categorically." *Id*. The statute "thus goes beyond merely affecting the procedural privilege to proceed as a class action." *Id*. (quotation and citation omitted). "Rather, it alters the 'vested rights and liabilities of the parties' by heightening the mens rea required for defendants to be liable." *Id*. at *23–24 (citing *In re D.A.H.*, 142 S.W.3d at 273). The court in

Haney held that "[g]iven the generally substantive nature of the . . . statute and its heightened mens rea requirement—and in light of the presumption of prospective application" the statute does not apply retroactively. *Id*. at *24. This Court agrees and finds Section 29-34-215 does not apply retroactively.

C. Negligence

Under Tennessee law,

> [a] negligence claim requires proof of the following familiar elements: (1) a duty of care owed by the defendant to the plaintiff; (2) conduct by the defendant falling below he standard of care amounting to a breach of that duty; (3) an injury or loss; (4) causation in fact; and (5) proximate or legal cause.

Biscan v. Brown, 160 S.W.3d 462, 478 (Tenn. 2005). Defendant first argues that Plaintiffs' negligence claim should be dismissed because their allegations to support the element of breach are insufficient under *Iqbal*, 556 U.S. at 678. (Doc. 28 at 7.) Defendant specifically argues that Plaintiffs fail to plead "specific conduct other than being the victim of a crime" to support the "bald assertions" that Defendants breached the duty of care. (*Id*. at 7–8.) Defendant further argues Plaintiffs fail to plead injury resulting from the alleged delay in notification of the data breach. (*Id*. at 9.)

1. Breach of Duty

Courts in other circuits are not uniform on the level of specificity required at the pleading stage of data breach cases, particularly given the "asymmetry of information" generally present. *See Hummel v. Teijin Auto. Techs., Inc.*, No. 23-cv-10341, 2023 U.S. Dist. LEXIS 167438 at *14–18 (E.D. Mich. Sep. 20, 2023). But "[n]othing in *Iqbal* indicates that [the pleading] standard should be relaxed in data breach cases, nor in any of the multitude of cases where there is an asymmetry of information between plaintiff and defendant." *Id*. at *18.

In *Hummel* the court considered a negligence claim arising from a data breach nearly identical to the pending case. *See generally id*. There, the district court declined to rely on the plaintiff's list of "industry standards and conclusory statements" to find the plaintiff had sufficiently pleaded breach. *See id*. at *19–21 (finding that to infer that a breach had occurred whenever a cyberattack succeeded "would, in effect, create strict liability in data breach cases"); *accord In re Waste Mgmt. Data Breach Litig.*, No. 21cv6147 (DLC), 2022 U.S. Dist. LEXIS 32798, at *13 (S.D.N.Y. Feb. 24, 2022). Instead, the court considered the plaintiff's specific allegation that the defendant could have prevented the data breach "by properly securing and encrypting the folder, files, and or date fields" containing the plaintiff's PII and that the failure to do so created a foreseeable risk of harm. *Id*. at *20. Because the failure to encrypt data was a "specific factual allegation," the court found the plaintiffs had adequately pleaded a breach of duty. *Id*. at *21. However, the court found the allegation that the defendant disclosed the data breach less than two weeks after it occurred did not constitute a breach the plaintiffs did not plead facts to suggest the notification was "untimely or otherwise improper." *Id*. at *22.

Plaintiffs allege Defendant inadequately safeguarded Plaintiffs' PII by deviating from industry rules, regulations, and practices. (Doc. 24 ¶¶ 117, 123, 132.) They list recommendations and standards from public and private sources, which include generic advice such as "[i]mplement an awareness training program," "[s]et anti-virus and anti-malware programs to conduct regular scans automatically," and "[o]pen email attachments with caution." (*Id*. ¶¶ 125–26.) Plaintiffs do not specify which of these guidelines Defendant failed to implement, but instead provide a list of "acts and/or omissions" that state general conclusions such as "[f]ailing to adequately protect patients' [PII]," and "[f]ailing to test and assess the adequacy of its data security system." (*Id*. ¶ 134.) They also allege the "computer systems [were] in need of security upgrades" and Defendant

had "inadequate procedures for handling" cyber threats. (*Id*. ¶ 135.) Plaintiffs conclude the occurrence of the data breach demonstrates Defendant's failure to adequately implement the cited standards and regulations. (*Id*. ¶ 99.) However, to make this inference would substitute a strict liability standard for that of negligence. *See Hummel*, No. 23-cv-10341, 2023 U.S. Dist. LEXIS 167438 at *14.

Plaintiffs' more specific allegations are that "on information and belief" the information accessed in the breach was unencrypted and Defendant was delayed in "identifying and reporting the [d]ata [b]reach." (*Id*. ¶¶ 99, 174.) Plaintiffs also allege the cybercrime group Karakurk "exploits vulnerabilities or weak credentials of the computer network" and "uses off-the-shelf tools and applications, often native to the victim system, to meet its objectives." (Doc. 24 ¶ 98.)

Defendant does not move to dismiss Plaintiffs' negligence claim on the grounds that Defendant had no duty to timely notify Plaintiffs of the data breach. (*See generally* Doc. 28.) Accordingly, the Court does not consider that issue here.

Additionally, the Court finds Plaintiffs' claim that data was unencrypted to be sufficiently specific to survive a motion to dismiss on the breach of duty element. *See Hummel*, No. 23-cv-10341, 2023 U.S. Dist. LEXIS 167438 at *21. While the allegation about unencrypted data is stated "upon information and belief," the Court draws all reasonable inferences from the entire pleading in favor of Plaintiffs, including consideration of the facts plead about Karakurk's typical methods. *See Smith*, 988 F.3d at 885; *Gold Crest, LLC*, 525 F. Supp. 3d at 837 n.10. The Court accepts Plaintiffs' allegation as true at this stage. *See Gunasekera*, 551 F.3d at 466. Plaintiffs allege facts sufficient to plead the negligence element of breach of duty.

2. Injury Resulting From Delayed Notification

Defendant argues that Plaintiffs fail to allege facts demonstrating they were harmed by Defendant's failure to timely disclose the data breach. (Doc. 28 at 9.) Plaintiffs respond that because they allege harm caused by the data breach and "post-disclosure remedial actions," they "raise an inference that timely disclosure would have prompted a swifter response and that the delay caused [] cognizable injury." (Doc. 31 at 15 (internal quotations omitted).) Defendant does not dispute that Plaintiffs plausibly allege the existence of a duty to make a timely notification or the breach of that duty. (*See id*. at 6–9.)

In *Allen v. Wenco Mgmt., LLC*, 696 F. Supp. 3d 432 (N.D. Ohio 2023) the court considered "whether a privacy injury is cognizable in negligence." *Id*. at 437. The district court noted that "other jurisdictions are split on the issue." *Id*. (comparing *Medoff v. Minka Lighting, LLC*, 2023 U.S. Dist. LEXIS 81398, 2023 WL 4291973, at *9 (C.D. Cal. May 8, 2023) (dismissing data-breach plaintiff's negligence claim because alleged "privacy injury" was "conclusory and vague" and thus not cognizable under California law) *with Mehta v. Robinhood Fin. LLC*, 2021 U.S. Dist. LEXIS 253782, 2021 WL 6882377, at *6 (N.D. Cal. May 6, 2021) (holding that data-breach plaintiffs alleged cognizable damages based on "harm to their privacy") *and Flores-Mendez v. Zoosk, Inc.*, 2021 U.S. Dist. LEXIS 18799, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021) (finding "loss of privacy with respect to highly sensitive information" to be a cognizable harm)). The court in *Allen* looked to cases considering injury in fact with regard to federal standing because the injury doctrine "is closely related to damages." *Id*. at 437.

In *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016), the court held that "allegations of a substantial risk of harm, coupled with reasonably incurred mitigations costs, are sufficient to establish a cognizable Article III injury at the pleading stage of litigation." *Id*. at

388. "Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in [the p]laintiffs' complaints." *Id.* Following *Galaria*, the Supreme Court decided *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), where it held "the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless exposure to the risk of future harm itself causes a *separate* concrete harm." *Id*. at 415 (emphasis in original). *Allen,* which was decided after *TransUnion*, found a privacy injury resulting from a data breach was "sufficiently concrete for Article III purposes." 696 F. Supp. 3d at 437. The court held the plaintiff's "alleged increased risk of identity theft" from the data breach gave him standing, which suggested it would also be considered an injury cognizable in negligence under state law. *Id*. at 438.

In the context of claims specifically arising from a delayed data breach notification, courts have held that "[p]laintiffs must allege 'incremental harm suffered as a result of the alleged delay in notification,' as opposed to harm from the [d]ata [b]reaches themselves." *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 U.S. Dist. LEXIS 140212, at *145–46 (N.D. Cal. Aug. 30, 2017) (considering whether plaintiff demonstrated an injury in fact to establish standing) (quoting *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *7 (S.D. Cal. Nov. 3, 2016)). In *Foster v. Health Recovery Servs.*, 493 F. Supp. 3d 622 (S.D. Ohio 2020), the plaintiff alleged the defendant's failure to timely notify of a data breach "resulted in financial injuries," but did not "allege what specific financial injury he suffered" from the delay. *Id*. at 630. The district court found the plaintiff failed to establish standing because he did not demonstrate an injury. *Id*. at 630–31 (citing *Savidge v. Pharm-Save, Inc.*, 3:17-CV-00186-TBR, 2017 U.S. Dist. LEXIS 197635, 2017 WL 5986972, at *8 (W.D. Ky. Dec. 1, 2017) ("This mere allegation of harm,

without accompanying factual allegations, is insufficient to warrant an inference that the alleged delay in notifying Plaintiffs of the security breach caused them cognizable injury."); *In re Adobe Sys., Inc. Priv. Litig.*, 66 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014) ("Plaintiffs have not alleged any injury traceable to Adobe's alleged failure to reasonably *notify* customers of the 2013 data breach ... because Plaintiffs do not allege that they suffered any incremental harm as a result of the delay."); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 3:19-CV-2284-H-KSC, 2020 U.S. Dist. LEXIS 80736, 2020 WL 2214152, at *8 (S.D. Cal. May 7, 2020) ("To allege a 'cognizable injury' arising from Defendant's alleged failure to timely notify Plaintiffs of the Data Breach, Plaintiffs must allege 'incremental harm suffered as a result of the alleged delay in notification,' as opposed to harm from the Data Breach itself.")).

The court in *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014) also considered whether the alleged injury from a delayed data breach notification was sufficient to satisfy the harm element of negligence. There, the plaintiffs alleged that "timely disclosure of the breach would have allowed Plaintiffs to take appropriate measures to avoid unauthorized charges . . ., cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks . . . , obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by [defendant's] misconduct." *Id*. at 1171 (internal quotations omitted). The district court found the allegations were "not fatally insufficient," and constituted a "short and plain statement" as required by Federal Rule of Civil Procedure 8(a)(2). *Id*.

Plaintiffs allege "Defendant's delay in identifying and reporting the [d]ata [b]reach caused additional harm." (Doc. 24 ¶ 174.) They assert that in a data breach "[e]arly notification helps a victim . . . mitigate their injuries, and . . . delayed notification causes more harm and increases the

risk of identity theft." (*Id.*) Plaintiffs also detail protective measures taken after notification of the data breach, including monitoring their financial accounts for misuse. (*Id.* ¶ 171.) Two Plaintiffs allege more specific personal harm. Plaintiff Sidney Jackson alleges that since the data breach she experienced "identity theft and fraud, including a $14 fraudulent charge on her credit card." (*Id.* ¶ 48.) This required her to order a new credit card. (*Id.*) Plaintiff Elyn Painter alleges that since the data breach she has received what appear to be fraudulent calls and text messages which she believes are related to the breach. (*Id.* ¶ 73.) She has spent time monitoring financial accounts and requesting a new debit card in response to the fraudulent communications. (*Id.* ¶ 75.)

At this stage, the Court draws all reasonable inferences in favor of Plaintiffs. During the time Plaintiffs were unaware that their data had been accessed in the breach, they were not yet spending time or money to mitigate the risk of harm. But Plaintiffs allege that the risk of identity theft was increased by the delay in notification. Consistent with *Galaria*, the Court infers that the cybercriminals who accessed Plaintiffs' data will use the data for fraudulent purposes. *See Galaria*, 663 F. App'x at 388. Privacy harm is a cognizable injury, as is an increased risk of identity theft. *Allen*, 696 F. Supp. 3d at 437–38. Any such harm that was increased by the notification delay is a harm attributable to the alleged breach of duty. Viewing the facts in the light most favorable to Plaintiffs, they sufficiently plead injury suffered as the result of the alleged delay. The Court need not opine on whether the specific instances of identity theft alleged by Plaintiffs Jackson and Painter can be attributed to the delay in notification. Plaintiffs allege facts sufficient to plead the negligence element of injury resulting from the alleged delay in notification.

Defendant's motion to dismiss Plaintiffs' negligence claim will be **DENIED.**

D. Negligence Per Se

Under Tennessee law, the elements of negligence per se are: (1) a violation of a statutory or regulatory duty of care; (2) a showing that the statute or regulation was meant to benefit and protect the injured party; and (3) proximate cause. *Steinberg v. Luedtke Trucking, Inc.*, No. 4:17-CV-9, 2018 U.S. Dist. LEXIS 109740, at *8 (E.D. Tenn. July 2, 2018) (citing *Chase, Jr. v. Physiotherapy Assocs., Inc.*, No. 02A01-9607-CV-00171, 1997 Tenn. App. LEXIS 608 (Tenn. Ct. App. Sept. 5, 1997)). "The negligence per se doctrine does not create a new cause of action." *Rains v. Bend of the River*, 124 S.W.3d 580, 589 (Tenn. Ct. App. 2003) (citations omitted). Instead, "it is a form of ordinary negligence that enables the courts to use a penal statute to define a reasonably prudent person's standard of care." *Id.* (citations omitted). But "[n]ot every statutory violation amounts to negligence per se." *Id*. at 590 (citation omitted). "To trigger the doctrine, the statute must establish a specific standard of conduct." *Id*. (citations omitted). Among other factors, courts must consider "whether the statute clearly defines the prohibited or required conduct." *Rains*, 124 S.W.3d at 591.

Plaintiffs claim Defendant violated the statutory standards of care under (1) Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45; (2) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, § 264, 110 Stat. 1936 (1996); (3) the Georgia Fair Business Practices Act ("GFBPA"), Ga. Code §§ 10-1-390 et seq.; and (4) the Tennessee Consumer Protection Act of 1977 ("TCPA"), Tenn. Code Ann. §§ 47-18-101 *et seq.* (Doc. 24 at 49.) Defendant moves to dismiss Plaintiffs' negligence per se claim on the grounds that none of the statutes at issue establish a specific standard of conduct. (Doc. 28 at 9.)

1. FTC Act

Section 5 of the FTC Act provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1). Plaintiffs reference materials promulgated by the FTC to define the standard of care required of Defendant, rather than the FTC Act itself. (*See* Doc. 24 ¶¶ 114–16, 145.) Plaintiffs specifically claim that "Defendant violated . . . FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards . . . ." (*Id*. ¶ 232.) Plaintiffs' reliance on extra-statutory FTC guidance indicates a concession that the statute does not define a standard of care and cannot support a negligence per se claim. *See In re HCA Healthcare, Inc. Data Sec. Litig.*, No. 3:23 CV 684, 2024 U.S. Dist. LEXIS 146929, at *24 (M.D. Tenn. Aug. 15, 2024) (holding the plaintiffs' reliance on "extra-statutory sources to determine what constitutes an 'unfair' cybersecurity practice . . . implicitly concede[d] that the statute itself provides no such answer." (quoting *Allen*, 696 F. Supp. at 440) (noting the FTC Act does not set forth a definite standard of care required to support a negligence per se claim)). Plaintiffs fail to state a claim for negligence per se under the FTC Act.

2. HIPAA

Plaintiffs rely on two HIPAA provisions for their negligence per se claim. (Doc. 24 ¶¶ 229–30.) First, Plaintiffs cite 45 CFR § 164.530(c), which requires covered entities to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." Second, Plaintiffs cite 45 CFR § 164.404, which states that a covered entity must provide notification of a breach of unsecured protected health information

"without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." (Doc. 24 ¶ 230.)

In order for a statute to create a standard of care, it must set "forth 'particular acts [that] shall or shall not be done,' so as to 'fix' a particular standard of care, for purposes of stating a negligence *per se* claim." *Doe v. Piraino*, 688 F. Supp. 3d 635, 665 (M.D. Tenn. 2023). The court in *Piraino* distinguished between provisions "relevant to the creation of a duty" from provisions that "'establish a specific standard of conduct,' aside from 'reasonableness.'" *Id.* (quoting *Rains*, 124 S.W.3d at 589)). The district court held that the statute at issue requiring promotion of a safe environment free from abuse of athletes stated general intent, but did not create a standard of care. *Id*. (citing *Rains*, 124 S.W.3d at 589).

The HIPAA provision requiring covered entities to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" does not state specific acts that are required or prohibited. 45 CFR § 164.530(c). Rather, like the statute at issue in *Piraino*, the provision states general intent and is "relevant to the creation of a duty," but does not create a standard of care. *See Piraino*, 688 F. Supp. 3d at 665.

The Court turns next to Plaintiffs' claim under the HIPAA breach notification provision. "Where a statutory provision does not define a standard of care but merely imposes an administrative requirement, such as the requirement to obtain a license or to file a report to support a regulatory scheme, violation of such requirement will not support a negligence per se claim." *King v. Danek Med.*, 37 S.W.3d 429, 460 (Tenn. Ct. App. 2000). This applies "[e]ven if the regulatory scheme as a whole is designed to protect the public or to promote safety, the licensing duty itself is not a standard of care, but an administrative requirement." *Id.* In *Ladd v. Nashville Booting, LLC*, No. 3:20-cv-00626, 2021 U.S. Dist. LEXIS 144967 (M.D. Tenn. Aug. 3, 2021), the

plaintiffs claimed negligence per se under an ordinance providing "that it is unlawful to fail to remove a boot within one hour after being contacted by the vehicle's owner." *Id*. at *14 (quoting Nashville Ordinance § 6.81.170(E)). There the court found there was no showing that the ordinance expressed a reasonable person standard that should replace the more general common law standard. *Id*. at *19–20. The court dismissed the negligence per se claim because the allegations under the ordinance could not support the action. *Id*. at *20.

The HIPAA requirement to provide notification of a breach states references the common law negligence standard of "reasonableness." *See* 45 CFR § 164.404 (stating that notification must be made "without unreasonable delay"). The breach notification provision is part of a regulatory scheme "designed to protect the public." *See King*, 37 S.W.3d at 460. But the sixty-day deadline, like the ordinance at issue in *Ladd*, is an administrative requirement that cannot support a negligence per se claim. *See Ladd*, No. 3:20-cv-00626, 2021 U.S. Dist. LEXIS 144967 at *20.

HIPAA does not create a statutory or regulatory duty of care relevant to Plaintiffs' negligence per se claim.

3. GFBPA and TCPA

Plaintiffs make negligence per se claims under Ga. Code Ann. § 10-1-393(b)(7) and Tenn. Code Ann. § 47-18-104(b)(7), which both provide it is a violation to represent that "goods or services are of a particular standard, quality or grade . . . if they are of another." Plaintiffs do not reference any other specific provisions of either statute in support of their claim. (*See generally* Docs. 24, 31.) The prohibition on representing goods and services as a different quality or grade

than they are does not state a standard of care. *See Rains*, 124 S.W.3d at 590. Neither GFBPA nor TCPA create a statutory duty of care that can support Plaintiffs' negligence per se claim.

Plaintiffs fail to state a claim that is plausible on its face under the FTC Act, HIPAA, GFBPA or TCPA. Defendant's motion to dismiss Plaintiffs' negligence per se claim will be **GRANTED**.

E. Breach of Implied Contract

In Tennessee, the elements of breach of a contract implied in fact[2] ("implied contract") are (1) existence of an enforceable contract, (2) nonperformance amounting to a breach of the contract, and (3) damages caused by the breach of contract. *Bancorp South Bank, Inc. v. Hatchel*, 223 S.W.3d 223, 227 (Tenn. Ct. App. 2006). "[I]n order for a contract implied in fact to be enforceable, it must be supported by mutual assent, consideration, and lawful purpose." *Thompson v. Hensley*, 136 S.W.3d 925, 930 (Tenn. Ct. App. 2003). A contract "must result from a meeting of the minds of the parties in mutual assent to the terms." *Johnson v. Cent. Nat'l Ins. Co. of Omaha, Neb.*, 356 S.W.2d 277, 281 (Tenn. 1962) (citation omitted).

Defendants dispute only the first element, existence of an enforceable contract, on the grounds that "Plaintiffs allege no facts supporting mutual assent." (Doc. 28 at 16.) Specifically, Defendants argue that Plaintiffs "do not allege any specific actions taken by [Defendant] from which an agreement can be inferred." *Id.* Plaintiffs assert that by providing their PII, and Defendant accepting the information, "the parties mutually assented to implied contracts." (Doc. 24 ¶ 240.) More specifically they contend that the implied contract was formed when Defendant

[2] The second type of implied contract is a contract implied in law, which has the same elements as unjust enrichment under Tennessee law. *Compare* Thompson, 136 S.W.3d at 931 *with Freeman Indus., LLC v. Eastman Chem. Co.*, 172 S.W.3d 512, 525 (Tenn. 2005). The Court does not address contract implied in law here because Defendant moved separately to dismiss Plaintiffs' unjust enrichment claim. (*See* Doc. 24 at 52.)

provided medical services in consideration for Plaintiffs' PII. (*Id*. ¶ 241.) Plaintiffs allege the "implied contracts included an implicit agreement and understanding" that Defendant would safeguard their PII, delete PII once it was no longer needed, and notify Plaintiffs "within a reasonable amount of time" after a data breach. (*Id*. ¶ 240.)

In *Haney*, the court found an implied contract where the plaintiffs were employees bringing a breach of implied contract claim against their employer, alleging that they "were required to provide their private information to [the] [d]efendants as a condition of their employment." No. 2:23-cv-46, 2024 U.S. Dist. LEXIS 159245, at *34. "[S]everal courts in [the Sixth Circuit] have held that an implied contract is formed between an employer and employee when employees are required to provide personal information to their employer as a condition of their employment, and the resulting implied contract requires the employer to take reasonable steps to protect the employees' information." *Id*. at *33. (citing *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019) (holding that when the plaintiffs "as a condition of their employment [] had to provide personal information" to the defendant, the defendant "implicitly agreed to safeguard that information"); *Bowen v. Paxton Media Grp.*, No. 5:21-cv-143, 2022 U.S. Dist. LEXIS 162083, at *6, 2022 WL 4110319, at *2 (W.D. Kent. Sept. 8, 2022)). But outside the employer-employee context, some courts "have held that providing PII in exchange for services may create an implied contract to safeguard the PII," while others "have declined to find an implied contract under similar circumstances." *Mohsen v. Veridian Credit Union*, No. C23-2048-LTS-KEM, 2024 U.S. Dist. LEXIS 85288, at *22–24 (N.D. Iowa May 9, 2024) (collecting cases). The Court is unaware of any case applying Tennessee law to a breach of implied contract claim in a context factually similar to the pending case.

In *Lochridge v. Quality Temp. Servs.*, No. 22-cv-12086, 2023 U.S. Dist. LEXIS 113794 (E.D. Mich. June 30, 2023), a corporation providing job recruiting and staffing services collected PII from applicants which was accessed in a data breach. *Id*. at *2. The plaintiff, like here, argued he had provided the information to the defendant with the expectation that the defendant would safeguard it. *Id*. The district court relied on cases in the Court of Appeals for the Sixth Circuit where plaintiffs' implied contract claims arose from data breaches in the employer-employee context to

conclude that an implied contract had been formed between the corporation and applicants. *Id*. at *20. The court in *Lochridge* reasoned that the defendant required the plaintiff to provide personal information to utilize the defendant's services, "thereby creating an implied contract" that the defendant would protect his PII and timely notify the plaintiff in the event of a data breach. *Id*. The plaintiff's argument that the defendant did not protect his personal information or provide notification of the breach in a timely manner was sufficient to state a claim for breach of implied contract. *Id*.

Plaintiffs have pleaded conduct that plausibly forms the basis of a breach of implied contract claim. Plaintiffs allege they provided PII to Defendant as part of the exchange for medical services, thereby creating an implied contract to safeguard Plaintiffs' PII. (Doc. 24 ¶ 241.) Plaintiffs "did not provide the PII gratuitously but rather expected that it would be protected and they would receive medical services in return." *See id*. ¶ 240; *Mohsen*, No. C23-2048-LTS-KEM, 2024 U.S. Dist. LEXIS 85288, at *24. They allege the exchange benefitted Defendant in that receipt of Plaintiffs' PII increased Defendant's income from provision of medical services. (*See id*. ¶ 241.) Additionally, viewing the facts in the light most favorable to Plaintiffs, the Court finds they plead facts to support the element of nonperformance of the contract by failing to take specific

action such as encrypting data to adequately safeguard information. Plaintiffs also allege economic damage caused by the breach. (*Id*. ¶ 173.)

Plaintiffs state an implied contract claim that is plausible on its face. Defendant's motion to dismiss Plaintiffs' implied contract claim will be **DENIED.**

F. Unjust Enrichment

The elements of an unjust enrichment claim are: (1) "[a] benefit conferred upon the defendant by the plaintiff"; (2) "appreciation by the defendant of such benefit"; and (3) "acceptance of such benefit under such circumstances that it would be inequitable for him to retain the benefit without payment of the value thereof." *Wilson Bank & Tr. v. Consol. Util. Dist.*, No. M2021-00167-COA-R3-CV, 2022 Tenn. App. LEXIS 228, at *26–27 (Ct. App. June 10, 2022) (quoting *Paschall's, Inc. v. Dozier*, 219 Tenn. 45, 407 S.W.2d 150, 155 (Tenn. 1966)). "The most significant requirement of an unjust enrichment claim is that the benefit to the defendant be unjust." *Id*.

Plaintiffs argue two basis for unjust enrichment. (*See* Doc. 24 ¶¶ 249–50.) The first is that PII has inherent value and Plaintiffs consequently "conferred a monetary benefit on Defendant" by giving Defendant their PII. (*Id*. ¶¶ 170, 249.) The second is that "Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure" the information. (*Id*. ¶ 250.) Specifically, Plaintiffs allege "Defendant was aware of the benefit conferred when it failed to provide reasonable security measures, instead calculating to avoid their data security obligations to Plaintiffs." (Doc. 31 at 25.)

In nearly identical circumstances the district courts in both *Haney* and *Lochridge* held the plaintiffs' allegations failed to satisfy the first element of unjust enrichment, that a benefit was conferred upon the defendant by the plaintiff. *Haney*, No. 2:23-cv-46, 2024 U.S. Dist. LEXIS

159245, at *34–35; *Lochridge*, 2023 U.S. Dist. LEXIS 113794, 2023 WL 4303577, at *6–7; *see also Tate v. EyeMed Vision Care, LLC*, No. 1:21-cv-36, 2023 U.S. Dist. LEXIS 175840, at *8 (S.D. Ohio Sep. 29, 2023); *Kingen v. Warner Norcross + Judd LLP*, No. 1:22-cv-01126, 2023 U.S. Dist. LEXIS 222175, at *4 (W.D. Mich. Sep. 28, 2023). In *Haney*, the court distinguished the value of the PII provided to the defendants in an employment context from "[c]onsumer information," which "has monetary value to a company [because] armed with such information, the company can target marketing at specific customers or sell the information to a third party who will do the same." No. 2:23-cv-46, 2024 U.S. Dist. LEXIS 159245, at *35. Unlike consumer information, plaintiffs' PII "only dealt with their identities and lacks value for non-illicit uses, such as using this data to market or selling the data to third parties." *Id*. In this case, Plaintiffs do not allege facts showing that Defendant commoditized, gained monetary benefit, or otherwise profited from Plaintiffs' PII, except to the extent it allowed Defendant to provide Plaintiffs with the medical services they purchased. (*See generally* Doc. 24.)

Additionally, Plaintiffs specifically allege they provided Defendant with their PII "in exchange for medical treatment." (Doc. 24 ¶ 249.) Assuming Plaintiffs received the medical services purchased, Defendants received no unaccounted-for benefit from the provision of PII that could sustain an unjust enrichment claim. (*See e.g.*, *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1249 (D. Colo. 2018) ("Plaintiffs paid for burritos; Plaintiffs received burritos."); *EyeMed Vision Care, LLC*, 2023 WL 6383467, at *8 (S.D. Ohio Sept. 29, 2023) ("Plaintiffs got what they paid for—vision benefits."); *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) ("[P]laintiff did not pay for a side order of data security and protection"); *In re SuperValu, Inc.*, 925 F.3d 955, 966 (8th Cir. 2019) ("Because [plaintiff] does not allege that any specific portion of his payment went toward data protection, he has not

alleged a benefit conferred in exchange for protection of his personal information nor has he shown how SuperValu's retention of his payment would be inequitable")).

Plaintiffs' second theory is that Defendant was enriched by the cost-savings of not paying for better cybersecurity. (Doc. 24 ¶ 250.) "A benefit is any form of advantage that has a measurable value including the advantage of being saved from an expense or loss." *Freeman Indus. LLC v. Eastman Chem. Co.,* 172 S.W.3d 512, 525 (Tenn. 2005) (citing *Lawrence Warehouse Co. v. Twohig*, 224 F.2d 493, 498 (8th Cir. 1955)). But "it is not simply the 'enrichment of the defendant [that is dispositive], but the *unjust* enrichment of the defendant at the expense of the plaintiff that is required to establish an unjust enrichment claim.'" *Cole v. Caruso*, No. W2017-00487-COA-R3-CV, 2018 Tenn. App. LEXIS 146, at *13 (Ct. App. Mar. 20, 2018) (quoting *Reprise Capital Corp. v. Rogers Group Inc.*, 802 S.W.2d 608, 610 (Tenn. Ct. App. 1990) (emphasis in original)).

The court in *Lochridge* rejected the argument that cybersecurity cost savings satisfied the first element of unjust enrichment because Michigan requires that a defendant "received a benefit directly from the plaintiff." No. 22-cv-12086, 2023 U.S. Dist. LEXIS 113794, at *18. In Tennessee, an indirect benefit can support a claim for unjust enrichment unless the benefit is "too attenuated." *Wilson Bank*, No. M2021-00167-COA-R3-CV, 2022 Tenn. App. LEXIS 228, at *27–28. Viewing the facts in the light most favorable to Plaintiffs and making reasonable inferences, Plaintiffs plausibly plead Defendant would have incurred additional cost had they invested in cybersecurity sufficient to prevent the data breach. But even accepting this as true, Defendant was not unjustly enriched at Plaintiffs' expense. Plaintiffs paid for the medical services received and there was no unaccounted-for benefit to form the basis of the alleged unjust enrichment. *See*

Caruso, No. W2017-00487-COA-R3-CV, 2018 Tenn. App. LEXIS 146, at *13; *SuperValu*, 925 F.3d at 966.

Plaintiffs do not allege facts showing Defendants received a benefit from receipt of Plaintiffs' PII. Accordingly, Defendant's motion to dismiss Plaintiffs' unjust enrichment claim will be **GRANTED.**

G. Bailment

Under Tennessee law, "[a] bailment is a delivery of personalty for a particular purpose or on mere deposit, on a contract expressed or implied, that after the purpose has been fulfilled it shall be re-delivered to the person who delivered it or otherwise dealt with according to his direction or kept until he reclaims it." *Aegis Investigative Grp. v. Metro. Gov't of Nashville & Davidson Cty.*, 98 S.W.3d 159, 162–63 (Tenn. Ct. App. 2002). "[B]ailees are not owners of the property, but merely temporary possessors." *Meade v. Paducah Nissan, LLC*, No. M2021-00563-COA-R3-CV, 2022 Tenn. App. LEXIS 225, at *11 (Ct. App. June 9, 2022) (citations omitted). "A bailment relationship is generally founded on a contractual relation; however, 'an actual contract or one implied in fact is not always necessary to create a bailment.'" *Akers v. Prime Succession of Tenn., Inc.*, 387 S.W.3d 495, 510 (Tenn. 2012) (quoting *Aegis Investigative Grp*, 98 S.W.3d at 163. "In the absence of express contract, the creation of a bailment requires that possession and control pass from bailor to bailee; there must be full transfer, actual or constructive, so as to exclude the property from the possession of the owner and all other persons and give the bailee sole custody and control for the time being." *Merritt v. Nationwide Warehouse Co.*, 605 S.W.2d 250, 253 (Tenn. Ct. App. 1980) (citation omitted).

Personal information is intangible and transfer of PII to one party does not limit transfer to another party. Plaintiffs do not plausibly allege they delivered PII to Defendant's exclusive

control, or that they transferred custody of their PII with the expectation that Defendants would deliver it back to them. Plaintiffs fail to state a claim for bailment. Defendant's motion to dismiss Plaintiffs' bailment claim will be **GRANTED.**

H. Breach of Fiduciary Duty

The elements of a breach of fiduciary duty are (1) a fiduciary relationship; (2) breach of the resulting fiduciary duty; and (3) injury to the plaintiff or benefit to the defendant as a result of that breach." *Ann Taylor Realtors, Inc. v. Sporup*, No. W2010-00188-COA-R3-CV, 2010 Tenn. App. LEXIS 755, at *9 (Ct. App. Dec. 3, 2010). In Tennessee, one category of fiduciary relationship is fiduciary *per se*, such as between a guardian and ward or attorney and client. *Foster Bus. Park, LLC v. Winfree*, No. M2006-02340-COA-R3-CV, 2009 Tenn. App. LEXIS 45, at *38 (Ct. App. Jan. 15, 2009). Another category, "often called a 'confidential relationship,'" "arise[s] in situations where one party exercise[s] 'dominion and control over another.'" *Id*. at *39 (quoting *Kelley v. Johns*, 96 S.W.3d 189, 197 (Tenn. Ct. App. 2002)). "Relationships that are not fiduciary *per se* 'require proof of the elements of dominion and control in order to establish the existence of a confidential relationship.'" *Id*. (quoting *Kelley*, 96 S.W.3d at 197). "[A] confidential relationship cannot be unilateral, rather both parties must understand that a special trust or confidence has been reposed." *Id*. (citations omitted).

"It is axiomatic that the physician-patient relationship is a fiduciary one." *Hammonds v. Aetna Cas. & Sur. Co.*, 237 F. Supp. 96, 102 (N.D. Ohio 1965); *see Shadrick v. Coker*, 963 S.W.2d 726, 736 (Tenn. 1998). "The policy of the law is to promote a full and free disclosure of all information by the patient to his treating physician; this information entrusted to the doctor creates a fiduciary responsibility in regard to that information." *Hammonds*, 237 F. Supp. at 102. But not all relationships between patients and medical service providers are fiduciary in nature. *See*

Hanger Prosthetics & Orthotics E., Inc. v. Kitchens, 280 S.W.3d 192, 195–96 (Tenn. Ct. App. 2008). In *Hanger*, the court found the relationship between an orthotist and patient did not rise to the level of a fiduciary relationship because "the orthotist role is more akin to providing goods and services." *Id*. at 196. Specifically, "unlike doctors and attorneys, patients rarely, if ever, choose the orthotist," and the orthotist's function is effectively to fill prescriptions written by doctors. *Id*. at 195. "[A]bsent extraordinary circumstances, parties dealing at arm's length in a commercial transaction lack the sort of relationship of trust and confidence that gives rise to a fiduciary relationship." *Dick Broad. Co. v. Oak Ridge FM, Inc.*, 395 S.W.3d 653, 673 (Tenn. 2013) (citations omitted).

Plaintiffs assert they entrusted Defendant with personal information to be safeguarded and argue they had a medical provider-patient relationship that was fiduciary in nature. (Doc. 31 at 27–28.) Defendant is not a doctor, but rather a healthcare service provider company. Plaintiffs do not allege there was a dynamic of dominion or control in the relationship between the parties. *See Foster*, No. M2006-02340-COA-R3-CV, 2009 Tenn. App. LEXIS 45, at *39. They also do not allege facts to suggest Defendant was aware of the existence of a relationship of special trust or confidence. *See id*. The dynamic between the parties was not one of doctor-patient confidentiality, but was effectively a commercial transaction in which Plaintiffs purchased medical services from Defendant. *See Hanger*, 280 S.W.3d at 195–96. Plaintiffs do not plead facts to support the existence of a fiduciary relationship. Defendant's motion to dismiss Plaintiffs' breach of fiduciary duty claim will be **GRANTED.**

I. Invasion of Privacy

Invasion of privacy is an intentional tort. *Meeks v. Gasaway*, No. M2012-02083-COA-R3-CV, 2013 Tenn. App. LEXIS 843, at *19 (Ct. App. Dec. 30, 2013). Plaintiff has brought two types

of invasion of privacy claims. First, Plaintiffs assert Defendant invaded their privacy by "publicizing" private facts. Second, Plaintiffs argue Defendant unreasonably intruded upon the seclusion of their private affairs. While the Tennessee Supreme Court has never expressly recognized that a cause of action exists for the public disclosure of private facts, Tennessee courts of appeal have recognized this tort." *Hoffman v. GC Servs. Ltd. P'ship.*, No. 3:08-cv-255, 2010 U.S. Dist. LEXIS 139509, at *57 (E.D. Tenn. Mar. 3, 2010).

A claim for public disclosure of private facts requires a plaintiff to "show that another person gave 'publicity' to a matter concerning plaintiff's private life. *Id*. at *58 (quoting *Beard v. Akzona, Inc.*, 517 F. Supp. 128, 132 (E.D. Tenn. 1981)). "'[P]ublic disclosure' must be understood in a particularized sense. *Id*. (citation omitted). "This means '[c]ommunication to a single individual or to a small group of people, absent . . . [a] confidential relationship, will not give rise to liability.'" *Id*. (quoting *Beard*, 517 F.Supp. at 132). The term "publicity" "means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Beard*, 517 F. Supp. at 133 (E.D. Tenn. 1981).

Plaintiffs allege Defendant's information technology network was subject to a cyberattack. They do not allege Defendants communicated their data to the public at large, or that they did so intentionally. Plaintiffs do not allege facts to support the theory of public disclosure of private facts.

The elements of unreasonable intrusion upon the seclusion of private affairs are "(1) an intentional intrusion, physical or otherwise; (2) upon the plaintiff's solitude or seclusion or private affairs or concerns; (3) which would be highly offensive to a reasonable person." *McClanahan v. Medicredit, Inc.*, No. 3:19-cv-00163, 2020 U.S. Dist. LEXIS 196544, at *29–30 (M.D. Tenn. Oct.

22, 2020) (quoting *Teno v. Iwanski*, 464 F. Supp. 3d 924, 2020 U.S. Dist. LEXIS 95478, 2020 WL 2843217, at *9 (E.D. Tenn. 2020)). In the context of procurement of financial or medical information, there is no intrusion if the information was not procured through improper means. *Id*. at *30 (citation omitted).

Plaintiff makes no factual allegations that Defendant procured their information by improper means. To the contrary, Plaintiffs describe giving their PII to Defendant "for safeguarding." (Doc. 24 at 56.) Plaintiffs' factual allegations do not support the theory of unreasonable intrusion upon the seclusion of private affairs.

Defendant's motion to dismiss Plaintiffs' claim for invasion of privacy will be **GRANTED.**

J. Declaratory and Injunctive Relief

Count eight of Plaintiffs' consolidated complaint is a freestanding claim seeking declaratory judgment against Defendant. (*See* Doc. 24 ¶¶ 59–60.) Under the Declaratory Judgment Act, a court may issue declaratory judgment in "case[s] of actual controversy." 28 U.S.C. § 2201(a). The Declaratory Judgment Act is merely a remedy and does not provide an independent standalone cause of action. *Davis v. United States*, 499 F.3d 590, 594 (6th Cir. 2007) (citing *Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950)).

> In considering whether to grant declaratory relief courts should consider: (1) whether the declaratory action would settle the controversy; (2) whether the declaratory action would serve a useful purpose in clarifying the legal relations in issue; (3) whether the declaratory remedy is being used merely for the purpose of "procedural fencing" or "to provide an arena for a race for res judicata;" (4) whether the use of a declaratory action would increase friction between our federal and state courts and improperly encroach upon state jurisdiction; and (5) whether there is an alternative remedy which is better or more effective.

Larry E. Parrish P.C. v. Bennett, 989 F.3d 452, 457 (6th Cir. 2021) (citing *Grand Trunk W. Rail Co. v. Consolidated Rail Corp.*, 746 F.2d 323, 326 (6th Cir. 1984)).

Before considering the five factors, courts must consider "whether the basic jurisdictional requirements have been met, such as whether the plaintiff has demonstrated standing for each claim and for each form of relief sought." *Hummel*, No. 23-cv-10341, 2023 U.S. Dist. LEXIS 167438, at *38 (citing *Lochridge*, 2023 U.S. Dist. LEXIS 113794, 2023 WL 4303577 at *8). When, as here, "the alleged injury is a future injury 'the plaintiff must demonstrate that the threatened injury is certainly impending or there is a substantial risk that the harm will occur.'" *Id*. (quoting *Lochridge*, 2023 U.S. Dist. LEXIS 113794, 2023 WL 4303577 at *8).

In *Hummel*, as here, the plaintiff stated claims for past injuries and potential future injuries. No. 23-cv-10341, 2023 U.S. Dist. LEXIS 167438, at *38–39. The court found the plaintiff's claim for declaratory judgment and injunctive relief "would not redress [the] injuries, rather, they seek to prevent a second breach from occurring." *Id*. at *39. Relying on *Lochridge*, the court in *Hummel* held that because the plaintiff did not allege facts to suggest a risk of a second cyberattack on the defendant, the plaintiff "failed to meet the jurisdictional requirements" for declaratory and injunctive relief. *Id*. (citation omitted). The same is true here.

Plaintiffs allege they "have an interest in ensuring that their [PII], which is believed to remain in the possession of Defendant, is protected from future breaches." (Doc. 24 ¶ 176.) They also argue "[t]here is no reason to believe that Defendant'[s] existing data security measures" are

more protective now than before the May 2023 data breach. (*Id.* ¶ 295.) But Plaintiffs do not allege specific facts regarding currently impending or substantial risk of another cyberattack on Defendant. (*See generally* Doc. 24.) Accordingly, Plaintiffs fail to meet the jurisdictional requirements for the relief requested. Defendant's motion to dismiss Plaintiff's claim for declaratory judgment and injunctive relief will be **GRANTED.**

IV. CONCLUSION

Defendant's motion to dismiss (Doc. 27) will be **GRANTED in part** and **DENIED in part**. The motion will be **DENIED** as to Plaintiffs' claims of negligence and breach of implied contract. The motion will be **GRANTED** as to all other claims. Plaintiffs' claims for negligence per se, unjust enrichment, bailment, breach of fiduciary duty, invasion of privacy, and declaratory judgment will be **DISMISSED WITH PREJUDICE**.

AN APPROPRIATE ORDER WILL ENTER.

/s/
CURTIS L. COLLIER
UNITED STATES DISTRICT JUDGE