UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FORT SMITH DIVISION

DAVID RODRIGUEZ, individually
and on behalf of all others similarly situated PLAINTIFFS

v. No. 2:23-cv-2002[1]

MENA HOSPITAL COMMISSION d/b/a
MENA REGIONAL HEALTH SYSTEM DEFENDANT

OPINION AND ORDER

Before the Court is Defendant Mena Hospital Commission's ("Mena") motion to dismiss and incorporated brief in support. (Doc. 47). Plaintiffs David Rodriguez, Jessica Smedley, P.S., A.S., Daniel Smedley, Tananda Smith, Chris Cant, Timothy Craig, and Carl Schoolfield ("Plaintiffs") filed a response in opposition. (Doc. 48). Mena replied. (Doc. 51). For the reasons given below, the motion will be GRANTED IN PART and DENIED IN PART.

I. Background

This case arises out of a data breach. Mena is a regional medical service provider located in Polk County, Arkansas. (Doc. 45, ¶ 26). Mena provides both inpatient and outpatient services. *Id.* Plaintiffs are all patients, or parents of patients, of Mena. *Id.* ¶ 33. To receive healthcare from Mena, Plaintiffs had to provide their personal information to Mena, including names, addresses, phone numbers, emails, dates of birth, Social Security numbers, insurance information, driver's licenses, and more. *Id.* Mena collects this information, and Mena also creates medical records for the patients that include protected health information. *Id.* ¶ 35. The Court will refer to this personally identifiable information and personal health information as "PII."

[1] Consolidated with Nos. 2:23-cv-2021, 2:23-cv-2023, 2:23-cv-2027, and 2:23-cv-2031.

On October 30, 2021, Mena was targeted by cybercriminals. *Id.* ¶ 1. These criminals accessed Mena's computer network and removed a number of files containing PII. *Id.* ¶ 2. In total, Plaintiffs allege the data breach affected 88,814 individuals. *Id.* ¶ 1. Mena investigated the incident and, over a year later, began notifying victims of the data breach that cybercriminals accessed the victims' PII. *Id.* ¶ 4. Mena did so by sending letters to patients notifying them of the data breach. *Id.* Plaintiffs attached examples of the letters to their complaint. *See* Doc. 45-2, pp. 2–4. Plaintiffs allege the cybercriminals took the following PII: "full names, dates of birth, Social Security numbers, driver's license/government identification numbers, financial account information, medical record/patient account numbers, medical diagnosis/treatment information, medical provider names, lab results, prescription information, and health insurance information." (Doc. 45, ¶ 3). Mena offered Plaintiffs a year of complimentary credit monitoring to help mitigate any consequences of the breach. *Id.* ¶ 48.

Plaintiffs allege that Mena's inadequate security practices led to the breach. *Id.* ¶ 37. Plaintiffs also allege that "Mena does not follow industry standard practices in securing patients' Private Information, as evidenced by the Data Breach." *Id.* ¶ 41. Plaintiffs' complaint includes over three pages of actions "Mena could and should have implemented." *See id.* ¶¶ 77–83. Plaintiffs drew these recommendations from the United States Government, the United States Cybersecurity & Infrastructure Security Agency, and the Microsoft Threat Protection Intelligence Team. *Id.* ¶¶ 78–80. Plaintiffs also cite studies about the value of PII, why healthcare organizations are targets of cyberattacks, and how long it takes victims of cyberattacks to resolve any problems resulting from the attacks. *See id.* ¶¶ 49–70.

Plaintiffs generally allege various injuries, including (1) diminished value of their PII, (2) out-of-pocket expenses associated with mitigating the effects of the data breach, (3) lost time and

opportunity mitigating the effects of the data breach, (4) loss of the benefits of their bargains with Mena, and (5) the ongoing increased risk to their PII, "which remains unencrypted and available for unauthorized third parties to access and abuse and may remain backed up in Mena's possession. . . ." *Id.* ¶ 12. Plaintiffs also allege each one of them "has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from [their] Private Information being placed in the hands of unauthorized third parties and possibly criminals." *Id.* ¶ 105; *see also id.* ¶¶ 116, 129, 142, 153, 164.

In addition to these general allegations, two of the named Plaintiffs have more specific allegations. First, David Rodriguez alleges that after the data breach he received a letter from a collection agency about a fraudulent account opened in his name. *Id.* ¶ 99. The collection agency claimed he owed $1,400. Mr. Rodriguez alleges this has impacted his credit score and required him "to spend significant time attempting to remediate the fraud." *Id.* Second, Carl Schoolfield alleges that after the data breach he received an unwanted package from Home Depot. *Id.* ¶ 110. He contacted Home Depot because he did not order the package. Home Depot stated a gift card was used to send the package to Mr. Schoolfield. Because the value of the package was of little value, Home Depot instructed Mr. Schoolfield to keep the package or throw it out. Home Depot said it would report the fraudulent purchase, and Mr. Schoolfield filed a police report about the fraudulent use of his home address. *Id.* Finally, three Plaintiffs also allege they have received increased spam texts or spam phone calls. *Id.* ¶¶ 117, 130, 159.

As a result of the data breach, the named Plaintiffs brought five lawsuits against Mena. The Court consolidated those actions and directed the Plaintiffs to file a consolidated amended complaint. (Doc. 28). In their consolidated class action complaint, Plaintiffs bring seven claims against Mena: (1) negligence, (2) breach of implied contract, (3) breach of fiduciary duty, (4)

unjust enrichment, (5) invasion of privacy, (6) declaratory judgment, and (7) violation of the Stored Communications Act, 18 U.S.C. §§ 2701–2713. (Doc. 45).

II. Legal Standard

In ruling on a motion to dismiss, the Court must "accept as true all facts pleaded by the non-moving party and grant all reasonable inferences from the pleadings in favor of the non-moving party." *Gallagher v. City of Clayton*, 699 F.3d 1013, 1016 (8th Cir. 2012) (quoting *United States v. Any & All Radio Station Transmission Equip.*, 207 F.3d 458, 462 (8th Cir. 2000)). "[A] complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotations omitted). Pleadings that contain mere "labels and conclusions" or "a formulaic recitation of the elements of the cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2009). However, "*Twombly* and *Iqbal* did not abrogate the notice pleading standard of Rule 8(a)(2). Rather, those decisions confirmed that Rule 8(a)(2) is satisfied 'when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Hamilton v. Palm*, 621 F.3d 816, 817 (8th Cir. 2010) (quoting *Iqbal*, 556 U.S. at 678). When, taken as true, the facts "raise a reasonable expectation that discovery will reveal evidence" to support a plaintiff's claim, the Court should deny a motion to dismiss. *Twombly*, 550 U.S. at 556.

III. Analysis

Mena has moved to dismiss all of Plaintiffs' claims for failure to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). The Court will address each claim in turn. The

parties and the Court agree that Arkansas law governs the state law claims. *See* Doc. 47, p. 12; Doc. 48, p. 11 n.2.[2]

A. Negligence

Plaintiffs allege that Mena was negligent in that Mena's inadequate security practices led to the breach. Doc. 45, ¶ 37. To state a claim for negligence under Arkansas law, Plaintiffs must allege Mena owes Plaintiffs a duty, Mena breached that duty, and Mena's breach was the proximate cause of Plaintiff's injuries. *Shanner v. United States*, 998 F.3d 822, 825 (8th Cir. 2021) (citing *Yanmar Co. v. Slater*, 386 S.W.3d 439, 449 (Ark. 2012)). The Court will decide if Mena owes Plaintiffs a duty because that is a question of law. *Id.* (citing *D.B. Griffin Warehouse Inc. v. Sanders*, 76 S.W.3d 254, 262 (Ark. 2002)).

Mena argues Plaintiffs cannot show (1) Mena owed any duty, (2) Mena breached any duty, or (3) Plaintiffs suffered any damages. (Doc. 47, p. 12). Plaintiffs assert Mena owes a duty under two theories. (Doc. 48, p. 12). First, they argue Mena owes a common law duty "based on the known risks that a failure to exercise due care would injure those who had entrusted their private information to Mena." *Id.* Second, Plaintiffs argue Mena owes a statutory duty to protect their PII under a negligence per se theory. *Id.* The Court will address each argument in turn.

1. Common Law Duty

"Duty is a concept that arises out of the recognition that relations between individuals may impose upon one a legal obligation for the other." *Yanmar*, 386 S.W.3d at 449 (citation omitted). Mena contends Plaintiffs are asking the Court to impose a new duty. (Doc. 47, p. 12). Mena describes this new duty as that of a hospital or health care entity "to protect its patients' PII from

[2] For consistency, all page references will be to the page number generated by the CM/ECF system rather than the document's internal numbering.

cyberattacks perpetrated by third party criminals." *Id.* Plaintiffs counter that they seek no new duty under Arkansas law, but rather they seek to apply the traditional negligence principle that a duty arises out of foreseeability. (Doc. 48, p. 12).

The parties have not cited, and the Court has not found, an Arkansas case on point with the facts of this case. In this instance, "[i]f Arkansas law is unclear on whether a duty is owed, we must do our best to predict how the Arkansas Supreme Court would rule in the circumstances." *I Square Mgmt., LLC v. McGriff Ins. Servs., Inc.*, 52 F.4th 1028, 1031 (8th Cir. 2022) (citation omitted). To aid in that prediction, the Court can "'look to relevant state precedent, analogous decisions, considered dicta, and any other reliable data to determine how the Supreme Court of [Arkansas] would construe [Arkansas] law.'" *Salier v. Walmart, Inc.*, 76 F.4th 796, 801 (8th Cir. 2023) (quoting *Ashley Cnty. v. Pfizer, Inc.*, 552 F.3d 659, 665 (8th Cir. 2009)). Also, "[i]t is not the role of a federal court to expand state law in ways not foreshadowed by state precedent." *Id.* at 802 (quoting *Ashley Cnty.*, 552 F.3d at 673). Based on a review of relevant caselaw from Arkansas courts, the Court predicts that Arkansas would recognize a common law duty here.

Arkansas courts recognize that "[t]he ultimate test in determining the existence of a duty to use due care is found in the foreseeability that harm may result if care is not exercised." *Shannon v. Wilson*, 947 S.W.2d 349, 352 (Ark. 1997); *see also Dancy v. Hyster Co.*, 127 F.3d 649, 654 (8th Cir. 1997) (explaining under Arkansas law, "negligence requires proof that an ordinarily prudent person in the same situation will foresee an appreciable risk of harm to others, causing him or her to act in a more careful manner."). In other words, "[t]he question . . . is not whether a defendant could have reasonably foreseen the exact or precise harm that occurred, or the specific victim of the harm . . . . It is only necessary that the defendant be able to reasonably foresee an appreciable

risk of harm to others." *Coca-Cola Bottling Co. of Memphis v. Gill*, 100 S.W.3d 715, 724 (Ark. 2003).

Plaintiffs allege that Mena should have been aware of the risk to Plaintiffs' PII because data breaches at healthcare providers are widely known. (Doc. 45, ¶¶ 57–66). Plaintiffs also allege the PII they provided Mena is valuable because it includes their Social Security numbers. *Id.* ¶¶ 51–56. In their brief, Plaintiffs argue that Mena's inadequate security measures made the data breach foreseeable, creating a duty to implement reasonable security measures. (Doc. 48, p. 13).

The Court agrees that there is a common law duty to act as a reasonably prudent health care entity to protect a patient's PII. Mena should be able to "reasonably foresee an appreciable risk of harm to others" if it has inadequate security measures. *Coca-Cola Bottling*, 100 S.W.3d at 724. This Court is far from the first court to recognize this duty in the data breach context. *See, e.g.*, *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *14 (D.N.J. Dec. 16, 2021) ("Once Defendants collected Plaintiffs' information, they had a duty to protect Plaintiffs from foreseeable harm by taking reasonable precautions to safeguard that information."); *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *8 (M.D. Fla. Jan. 27, 2020) (finding same); *In re Equifax, Inc. Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019) (finding same); *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1221 (11th Cir. 2023); *but see In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019) (no common law duty under Illinois law).[3] Based on the Plaintiffs' allegations, Mena owed them the same duty to take reasonable steps to safeguard that information.

[3] In *In re SuperValu*, the Eighth Circuit had the benefit of an Illinois Appellate Court decision that held Illinois "does not recognize a duty in tort to safeguard sensitive personal information." 925 F.3d at 963 (citing *Cooney v. Chi. Pub. Schs.*, 943 N.E.2d 23, 28–29 (Ill. App. Ct. 2010)). Mena does not cite an Arkansas case holding the same, so *In re SuperValu* is not binding authority.

Mena argues that Arkansas courts hold "defendants do not owe a duty of care to protect individuals from the criminal acts of third parties." (Doc. 47, p. 12) (citing *Boren v. Worthen Nat'l Bank of Ark.*, 921 S.W.2d 934, 938 (Ark. 1996)). Arkansas law is not so black and white. The *Boren* court explained that Arkansas has previously recognized several occasions where there is a "duty of a business owner to protect its patrons from criminal attacks . . . ." 921 S.W.2d at 940. Arkansas courts recognize that duty "where the [business] owner or its agent was aware of the danger presented by a particular individual or failed to exercise proper care after an assault had commenced." *Id.* The Arkansas Supreme Court has also recognized such a duty between an employment agency and a prospective employee because there was a contractual relationship between the parties, the agency could foresee some danger to the prospective employee, and the agency had some control over the employers available to the prospective employee. *See id.* (citing *Keck v. Am. Emp. Agency, Inc.*, 652 S.W.2d 2 (Ark. 1983)).

Neither *Boren* nor *Keck* is perfectly on point. *Boren* was a premises liability case concerning whether a bank owed a duty to its patron at an unmanned ATM machine. As discussed above, *Keck* involved whether an employment agency was liable to a prospective employee for the criminal acts of a third party—an employer sexually assaulting the employee. Thus, the Court is left to predict whether the Arkansas Supreme Court would recognize a duty here. The Court predicts that the Arkansas courts would recognize a duty because of the valuable information Plaintiffs provided Mena and the known risk that a healthcare provider would be subject to data breaches. This duty arises from the foreseeability of harm to Plaintiffs if Mena does not excise care in the safeguarding of Plaintiffs' PII. *See Shannon*, 947 S.W.2d at 352.

In sum, the Court does not tread new ground in recognizing a common law duty between the parties here. Under Arkansas law, Mena has a duty to use due care in the protection of

Plaintiffs' PII because of the "foreseeability that harm may result if care is not exercised." *Shannon*, 947 S.W.2d at 352. At this stage of the litigation, it is enough for the Court to conclude that Plaintiffs have alleged a common law duty that Mena owes, and Plaintiffs' claim will not be dismissed if they allege the other elements of a negligence claim.

2. Statutory Duty

Plaintiffs also allege Mena owes a duty created by statute on a negligence per se theory. (Doc. 48, p. 14). The two statutes Plaintiffs rely on are the Health Insurance Portability and Accountability Act ("HIPAA") and the Federal Trade Commission Act ("FTCA"). *Id.* at 15. While the Court was willing to recognize a common law duty, the Court will not recognize a duty imposed by statute.

"Under Arkansas law, the violation of a statute is only evidence of negligence and does not constitute negligence per se." *Cent. Okla. Pipeline, Inc. v. Hawk Field Servs., LLC*, 400 S.W.3d 701, 712 (Ark. 2012) (citing *Shannon*, 947 S.W.2d at 349). Plaintiffs are correct that the Arkansas Supreme Court has recognized a duty arising out of a statute, but in that case, the court did so "rely[ing] on the high duty of care that has been statutorily imposed on licensed alcohol vendors." *Id.* Plaintiffs have not explained how HIPPA or the FTCA have imposed a high duty of care on healthcare entities like Mena, so the Court does not think it wise to impose a separate duty based on the alleged violation of either statute.

The Court joins other federal courts in predicting the Arkansas Supreme Court would not recognize a common law duty created by federal statutes or regulations. *See, e.g.*, *Hammett v. Portfolio Recovery Assocs., LLC*, 2022 WL 3370912, at *35 (E.D. Ark. Aug. 16, 2022) ("the Court predicts that the Arkansas Supreme Court would not recognize a common-law duty in tort arising from the [Fair Debt Collection Practices Act.]"). As the Eighth Circuit has explained, "Arkansas

courts have been hesitant to permit Arkansas statutes and regulations to expand common law causes of action . . . and only do so when faced with clear legislative intent." *Chew v. Am. Greetings Corp.*, 754 F.3d 632, 637–38 (8th Cir. 2014) (citation omitted) (Occupational Safety and Health Administration regulations could not form alternative duty).

Based on this, the Court will not impose a duty based on statute. However, because the Court has recognized a common law duty, the Court will evaluate Mena's arguments about breach and damages.

3. Breach

Mena argues that Plaintiffs have not pled with specificity how Mena breached its duty. (Doc. 47, p. 13). In its reply, Mena argues that courts in data breach cases require plaintiffs to plead their claims with specificity. (Doc. 51, p. 6) (citing *In re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *5 (S.D.N.Y. Feb. 24, 2022)). Plaintiffs respond that Federal Rule of Civil Procedure 8 does not require them to plead their claims with specificity at this stage. The Court agrees with Plaintiffs. Until the Eighth Circuit says otherwise, Plaintiffs need only plead "'factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" *Hamilton*, 621 F.3d at 817 (quoting *Iqbal*, 556 U.S. at 678).[4]

Plaintiffs allege Mena "fail[ed] to implement industry protocols and exercise reasonable care in protecting and safeguarding" Plaintiffs' PII. (Doc. 45, ¶ 201). Plaintiffs also allege that

[4] The Eleventh Circuit has explained some of the challenges of pleading negligence claims in data breach cases. "[D]ata breach cases present unique challenges for plaintiffs at the pleading stage. A plaintiff may know only what the company has disclosed in its notice of a data breach. Even if some plaintiffs can find more information about a specific data breach, there are good reasons for a company to keep the details of its security procedures and vulnerabilities private from the public and other cybercriminal groups." *Ramirez*, 69 F.4th at 1220. The Court finds this analysis persuasive in support of its decision to not require Plaintiffs to plead every factual detail of the alleged negligence with specificity.

Mena failed to heed industry warnings, failed to have procedures in place to detect the disclosure of Plaintiffs' PII, and failed to remove PII Mena was no longer required to retain. *Id.* ¶¶ 203–05. Finally, as briefly discussed above, Plaintiffs allege Mena violated the FTCA and HIPAA. *Id.* ¶¶ 210, 213. Again, while those statutes cannot establish negligence per se, violations of those statutes could be evidence of negligence. *See Cent. Okla. Pipeline*, 400 S.W.3d at 712.

The Court finds that these allegations are sufficient to infer that Mena is liable for the alleged misconduct. This Court is not the first district court in the Eighth Circuit to allow negligence claims arising out of data breaches to proceed past the motion to dismiss stage. *See Perry v. Bay & Bay Trans. Servs., Inc.*, 2023 WL 171885, at *8 (D. Minn. Jan. 12, 2023) (applying Minnesota law). What's more, other district courts around the country have similarly allowed negligence claims in the data breach context to move forward. *See, e.g.*, *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1222–25 (S.D. Fla. 2022) (plaintiffs pled defendants "fail[ed] to exercise reasonable care" and "fail[ed] to safeguard and protect Plaintiffs' and Class Members' PHI and PII"); *In re Am. Med. Collection Agency*, 2021 WL 5937742, at *14–16; *In re Equifax*, 362 F. Supp. 3d at 1325. While perhaps a little thin, Plaintiffs' pleadings are sufficient to support a reasonable inference that Mena breached its duty. At this early stage, that is all that is required. As the case progresses, Plaintiffs will have to put on evidence of this alleged breach.

4. Damages

Mena lastly challenges Plaintiffs' ability to plead damages. (Doc. 47, p. 15). Plaintiffs group their alleged damages into four categories: "(1) the certainly impending and increased risk of identity theft and fraud; (2) lost time and expenses mitigating the effects of the Data Breach; (3)

diminished value of their [PII]; and (4) lost benefits of their bargains." (Doc. 48, p. 17); *see also* Doc. 45, ¶ 215.

The Court concludes that Plaintiffs have sufficiently alleged damages. Plaintiffs plead that they have suffered or will suffer actual identity theft, out-of-pocket expenses associated with mitigating the damage caused by the exposure of their information, lost time mitigating these same damages, and continued risk to their PII as the PII is still in Mena's hands. (Doc. 45, ¶ 215). Each named Plaintiff has also alleged the diminution of value in their PII. *Id.* ¶¶ 103, 114, 127, 140, 151, 162. Finally, two Plaintiffs have alleged specific misuses of their PII, and three Plaintiffs allege increased spam phone calls because of the breach. *Id.* ¶¶ 99, 110, 117, 130, 159.

Again, the Court joins other district courts in this circuit finding similar allegations are sufficient to plead damages in the data breach context. *See, e.g.*, *Hall v. Centerspace*, LP, 2023 WL 3435100, at *7–8 (D. Minn. May 12, 2023); *In re: Netgain Tech., LLC*, 2022 WL 1810606, at *13 (D. Minn. June 2, 2022) (collecting cases); *Baldwin v. Nat'l W. Life Ins. Co.*, 2021 WL 4206736, at *3–4 (W.D. Mo. Sept. 15, 2021). Although *Hall* analyzes Minnesota law, the Court finds that case particularly instructive.

In *Hall*, the court found the following allegations sufficient to plead damages: (1) the plaintiff's exposed PII placed him at risk for identity theft now and in the future, (2) the plaintiff's PII had diminished in value, (3) the plaintiff had to spend time monitoring his accounts, and (4) the defendant's untimely notification prevented the plaintiff from taking prompt action to protect his PII. 2023 WL 3435100, at *7. These allegations are nearly identical to those made here. Moreover, the *Hall* court also explained that "[a]lthough [the defendant] has pointed to cases in its briefing that have granted Rule 12(b)(6) motions based on insufficient damages claims, none are binding authority." *Id.* at *8. Here, Mena has similarly cited some cases where courts have granted

motions to dismiss, but none of those cases are binding on this Court. This Court instead joins *Hall* and numerous other courts in a trend of recognizing "the lost property value of personal information." *Id.* (quoting *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021)).

Mena has presented neither binding Eighth Circuit authority nor Arkansas caselaw suggesting that Plaintiffs' alleged damages cannot be recovered. As the Court explained in Section 3 above, Plaintiffs' pleadings are sufficient to support a reasonable inference that they are damaged. Plaintiffs will have the burden to prove those damages later in this case.

Based on the above analysis, Plaintiffs have adequately alleged duty, breach, and damages. Therefore, the Court will deny Mena's motion as it relates to the negligence claim.

B. Breach of Implied Contract

Plaintiffs' second claim is for breach of implied contract. Plaintiffs allege that they entered an implied contract with "Mena by which Mena agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen." (Doc. 45, ¶ 220). Plaintiffs allege Mena acknowledged its legal duty to protect Plaintiffs' PII in its Privacy Policy. *Id.* ¶¶ 28, 221. For their part, Plaintiffs allege they entrusted their PII to Mena to receive Mena's services. *Id.* ¶¶ 95, 107, 119, 124, 144, 155, 220, 222. Finally, Plaintiffs allege Mena breached the implied contract by failing to safeguard Plaintiffs' PII, failing to delete the PII after the parties' relationship ended, and failing to provide timely notice of the data breach. *Id.* ¶ 223.

"Under Arkansas law, implied contracts are 'inferred from the acts of the parties.'" *Air Evac EMS, Inc. v. USAble Mut. Ins. Co.*, 931 F.3d 647, 654 (8th Cir. 2019) (quoting *Steed v. Busby*, 593 S.W.2d 34, 38 (Ark. 1980)). Implied contracts "can be 'proven by circumstances showing the parties intended to contract or by circumstances showing the general course of dealing between

the parties.'" *Id.* Implied contracts require the same elements as express contracts, which are (1) competent parties, (2) subject matter, (3) legal consideration, (4) mutual agreement, and (5) mutual obligations. *Id.* (citing *Berry v. Cherokee Vill. Sewer, Inc.*, 155 S.W.3d 35, 38 (Ark. Ct. App. 2004)). Mena challenges Plaintiffs' ability to show consideration, mutual assent, or damages arising from the breach. (Doc. 47, p. 18).

Mena first argues Plaintiffs have not pleaded adequate consideration to support the implied contract. Under Arkansas law, "[c]onsideration is any benefit conferred or agreed to be conferred upon a promisor to which he is not lawfully entitled, or any prejudice suffered or agreed to be suffered by a promisee, other than that which he is lawfully bound to suffer." *Trakru v. Mathews*, 434 S.W.3d 10, 16 (Ark. Ct. App. 2014) (citing *Landmark Sav. Bank v. Weaver-Bailey Contractors, Inc.*, 739 S.W.2d 166 (Ark. Ct. App. 1987)). Mena distinguishes Plaintiffs' exchange of PII for Mena's medical services and Plaintiffs' alleged lack of consideration in exchange for protection of the PII. The Court does not see a reason to distinguish between these two exchanges. Plaintiffs have alleged that they exchanged their PII for medical services, and the Court joins others in recognizing that such a transaction includes a promise to protect the Plaintiffs' PII. *See, e.g.*, *Perry*, 2023 WL 171885, at *9; *Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1187 (M.D. Fla. 2022) ("The majority of federal courts have held that the existence of an implied contract to safeguard customers' data could reasonably be found to exist between a merchant and customer when a customer uses a payment card to purchase goods and services.") (quotation omitted). The Court finds that Plaintiffs have adequately plead consideration.

Mena next argues Plaintiffs have not pleaded mutual assent between the parties. Plaintiffs argue the agreement to protect data is implied in the parties' contract. Mena, conversely, argues that the parties never agreed to the protection of their PII as a condition of Plaintiffs receiving

medical services. Plaintiffs allege that "[i]n its Privacy Policy, Mena represented that it had a legal duty to protect Plaintiffs' and Class Members' [PII]." (Doc. 45, ¶ 221). Plaintiffs also cite multiple out-of-circuit cases where courts have recognized adequately pleaded implied contract claims between customers and merchants to safeguard customers' PII. *See* Doc. 48, pp. 22–23. This Court agrees with the others that have found an implied promise to safeguard PII when a merchant—here, a medical provider—requires the exchange of a customer's PII for services. *See, e.g.*, *Farmer*, 582 F. Supp. 3d at 1187.

This Court's decision is bolstered by the other district courts in this circuit which have allowed breach of implied contract claims to survive a motion to dismiss in the data breach context. *See, e.g.*, *Hall*, 2023 WL 3435100, at *5–6; *Perry*, 2023 WL 171885, at *9; *Baldwin*, 2021 WL 4206736, at *6–7; *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014). To be sure, other courts have reached contrary results. *See, e.g.*, *Ramirez*, 69 F.4th at 1221; *Baldwin*, 2021 WL 4206736, at *7 n.6 (collecting cases). However, none of those cases is binding here. The Court sees no reason to depart from the growing consensus among district courts in this circuit that allow breach of implied contract claims to survive a motion to dismiss in the data breach context.

Finally, Mena challenges Plaintiffs ability to show damages. That argument is rejected for the reasons stated above in the discussion of damages on Plaintiffs' negligence claim. Moreover, no party raised this issue, but "under Arkansas law, actual damage caused by the breach is not an essential element of a claim for breach of contract because a plaintiff is entitled to recover nominal damages in the absence of proof of actual damages." Ark. Model Jury Instruction 2401, *cmt*. (collecting cases). The cases collected in the commentary to the Model Jury Instruction explain that a breach can occur without causing damage, and in those instances, nominal damages are

appropriate. *See, e.g.*, *Blair v. U.S. ex rel. Gregory-Hogan*, 150 F.2d 676, 678 (8th Cir. 1945). Here, because the Court has found Plaintiffs have adequately pleaded damages and nominal damages are available if a breach did not cause actual damage, the Court rejects Mena's argument on damages.

This Court finds that Plaintiffs have adequately pleaded both consideration and mutual assent. Furthermore, the Court finds that Plaintiffs have pleaded damages to support their implied contract claim for the same reasons stated above in the negligence section. Therefore, the Court will deny Mena's motion as it relates to the implied contract claim.

C. Breach of Fiduciary Duty

Plaintiffs claim that Mena breached its fiduciary duty to Plaintiffs. As to the existence of the fiduciary relationship, Plaintiffs allege "[i]n providing their Private Information to Mena, Plaintiffs and Class Members justifiably placed a special confidence in Mena to act in good faith and with due regard for the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information." (Doc. 45, ¶ 227). Plaintiffs further allege that "Mena accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its acknowledgement that it had a legal duty to protect Plaintiffs' and Class Members' Private Information." *Id.* ¶ 228. Plaintiffs believe that Mena became a fiduciary because "Mena became a guardian of Plaintiffs' and Class Members' Private Information." *Id.* ¶ 229. Finally, Plaintiffs allege Mena breached the duty by failing to protect the integrity of its computer systems and failing to safeguard Plaintiffs' PII. *Id.* ¶¶ 231–32.

"[B]efore there can be a breach of a fiduciary duty, a fiduciary relationship must exist." *City of Prescott v. Sw. Elec. Power Co.*, 438 F. Supp. 3d 943, 953 (W.D. Ark. 2020). The existence of a fiduciary relationship is a question of law. *Long v. Lampton*, 922 S.W.2d 692, 698 (Ark.

1996). "A fiduciary relationship exists between two persons, one of whom has a duty to act for the benefit of another and owes the other duties of good faith, trust, confidence, and candor." *City of Prescott*, 438 F. Supp. 3d at 953 (quoting 1 HOWARD W. BRILL & CHRISTIAN H. BRILL, ARK. LAW OF DAMAGES § 15.3 (Nov. 2022 update)). Arkansas courts have recognized many fiduciary relationships, including between attorney and client,[5] guardian and ward,[6] manager and business,[7] and between business partners.[8] On the other hand, Arkansas has not recognized fiduciary relationships between a student with special needs and her school[9] or between a priest and parishioner.[10] Arkansas courts have not addressed whether a relationship exists between the parties here: health care systems and their patients. Again, because the Arkansas Supreme Court has not addressed this issue and because the Court sits in diversity, the Court's task is to predict how the Arkansas Supreme Court will rule. *Salier*, 76 F.4th at 801 (citation omitted).

The Court predicts the Arkansas Supreme Court would not recognize a fiduciary relationship between a healthcare system and its patients. Contracting parties in Arkansas do not necessarily owe each other fiduciary duties. *W. Memphis Adolescent Residential, LLC v. Compton*, 374 S.W.3d 922, 927 (Ark. Ct. App. 2010) (citing *Evans Indus. Coatings Inc. v. Chancery Ct. of Union Cnty.*, 870 S.W.2d 701, 703–04 (Ark. 1994)). Despite opposing the breach-of-implied-

[5] *Allen v. Allison*, 155 S.W.3d 682, 691 (Ark. 2004).

[6] *Hetrick v. Est. of Sams*, 670 S.W.3d 430, 434 (Ark. Ct. App. 2023).

[7] *Pennington v. Harvest Foods, Inc.*, 934 S.W.2d 485, 495 (Ark. 1996).

[8] *St. Joseph's Reg'l Health Ctr. v. Munos*, 934 S.W.2d 192, 197 (Ark. 1996) (citing *Boswell v. Gillett*, 295 S.W.2d 758 (Ark. 1956)).

[9] *Key v. Coryell*, 185 S.W.3d 98 (Ark. Ct. App. 2004).

[10] *Cherepski v. Walker*, 913 S.W.2d 761 (Ark. 1996).

contract claim, Mena acknowledged "Plaintiffs were clients of Mena, a health care system, and they engaged Mena to provide them with health care services." (Doc. 47, p. 18). But even this contractual relationship does not necessarily give rise to a fiduciary duty. *See Evans Indus. Coatings*, 870 S.W.2d at 704 (explaining that simply being a part of a contract does not create "a particular relationship of trust or confidence"). Nothing about the parties' relationship here takes it beyond the typical one between patient and healthcare system. This general rule supports the Court's prediction.

Analogous Arkansas precedent about fiduciary relationships between banks and customers illustrates the operation of this general rule. *See Quinn v. O'Brien*, 596 S.W.3d 20, 27 (Ark. Ct. App. 2020) (collecting cases). "Ordinarily, a bank and its customer hold a relationship of debtor and creditor." *Id.* Arkansas courts recognize fiduciary relationships between banks and customers in limited circumstances, such as "when [a] bank was appointed as attorney-in-fact for customer in construction-loan contract for purposes of making payments." *Id.* (citing *Knox v. Regions Bank*, 286 S.W.3d 737, 741 (Ark. Ct. App. 2008)). However, there is a high bar to prove such a fiduciary relationship, with a customer needing to show "the relationship is beyond that of debtor-creditor, and it takes more than a long-term relationship between the parties to meet this burden." *Id.* (citing *Farm Credit Midsouth, PCA v. Bollinger*, 548 S.W.3d 164 (Ark. Ct. App. 2018)).

The Court finds this precedent persuasive because of the similarities in the customer-bank and patient-healthcare system relationships. Like bank customers, patients must provide private information to the healthcare system. Like banks, healthcare systems acquire private information from many different patients. But as discussed above, not every bank-customer relationship transforms into a fiduciary relationship; there must be something more to transform the ordinary banking relationship into a fiduciary one. *Quinn*, 596 S.W.3d at 27.

The Court predicts the Arkansas Supreme Court would require a similar higher showing to transform the patient-healthcare system relationship into a fiduciary one. Plaintiffs describe Mena as being a guardian of its data, with the fiduciary relationship arising from Plaintiffs "justifiably plac[ing] a special confidence in Mena to act in good faith and with due regard for the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information." (Doc. 45, ¶ 227). These allegations, however, do not show any special relationship beyond what is typical of patients and healthcare systems. Because of this, the Court believes the analogous precedent about the bank-customer relationship supports its prediction that Arkansas would not recognize a fiduciary relationship here.

Plaintiffs point to a case from Ohio that recognized a fiduciary duty in the data breach context. *See Tucker v. Marietta Area Health Care, Inc.*, 2023 WL 423504, at *6 (S.D. Ohio Jan. 26, 2023). But unlike in Arkansas, "Ohio recognizes that medical providers . . . hold 'a fiduciary position' with patients and have a duty to keep patient's medical information confidential." *Id.* (citing *Herman v. Kratche*, 2006 WL 3240680, at *3 (Ohio Ct. App. 2006)). So even if the Ohio case arose from a similar data breach, the underlying state caselaw serves to distinguish *Tucker* here. The same is true of the other state court cases Plaintiffs cite from other jurisdictions. Moreover, this Court is far from the first to dismiss breach of fiduciary duty claims in the data breach context. *See, e.g.*, *Weisenberger v. Ameritas Mut. Holding Co.*, 597 F. Supp. 3d 1351, 1368 (D. Neb. 2022) (dismissing fiduciary duty claim on 12(b)(6) motion under Nebraska law).[11]

[11] *See also In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1145–46 (C.D. Cal. 2021) (dismissing claim under California law); *In re Mednax Servs.*, 603 F. Supp. 3d at 1226 (same under Florida law); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1202–03 (D. Or. 2016) (same under Washington law).

Based on the current state of Arkansas caselaw, the Court predicts that Arkansas would not recognize a fiduciary relationship between a healthcare system and its patients. Nothing in Arkansas's precedent foreshadows such an expansion of its caselaw, so it is not the role of this Court to expand state law. *See Salier*, 76 F.4th at 802. Therefore, the Court will dismiss Plaintiffs' claim for breach of fiduciary duty.

D. Unjust Enrichment

Plaintiffs also bring a claim for unjust enrichment in the alternative to their breach of implied contract claim. (Doc. 45, ¶ 236). Plaintiffs allege they "conferred a monetary benefit on Mena, by providing Mena with their valuable Private Information." *Id.* ¶ 237. They further allege "Mena enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information." *Id.* ¶ 238. "If Plaintiffs and Class Members knew that Mena had not secured their Private Information, they would not have agreed to provide their Private Information to Mena." *Id.* ¶ 242. Plaintiffs allege that Mena enriching itself by saving costs is unjust because "Mena should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Mena failed to implement appropriate data management and security measures that are mandated by industry standards." *Id.* ¶ 240.

"To be unjustly enriched under Arkansas law, 'a party must have received something of value, to which he or she is not entitled and which he or she must restore.'" *Friedman v. Farmer*, 788 F.3d 862, 866 (8th Cir. 2015) (quoting *Campbell v. Asbury Auto., Inc.*, 381 S.W.3d 21, 36 (Ark. 2011)). "The benefitted party must have acted or intended 'to make the enrichment unjust and compensable.'" *Id.* "In other words, a person must have 'received money or its equivalent under such circumstances that, in equity and good conscience, he or she ought not to retain.'" *Id.*

The Court cannot find, and the parties do not cite, any Arkansas caselaw discussing unjust enrichment claims in the data breach context.

The Eighth Circuit has considered unjust enrichment claims in the data breach context twice. *See In re SuperValu, Inc.*, 925 F.3d at 966 (applying Illinois law); *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 718 (8th Cir. 2017) (applying Missouri and Florida law). Both times, the Eighth Circuit affirmed dismissal of the claims. The court did so because the plaintiffs did not allege "a benefit conferred in exchange for protection of [their] personal information." *In re SuperValu*, 925 F.3d at 966; *see also Kuhns*, 868 F.3d at 718 (quoting *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 912 (8th Cir. 2016)). The *In re SuperValu* court went as far as to say "[c]ommon sense counsels against the viability of [plaintiff's] theory of unjust enrichment. . . . He did not pay a premium 'for a side order of data security and protection.'" 925 F.3d at 966 (quoting *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016)).

Plaintiffs argue instead that there is no requirement to itemize the amount paid for data security and in the alternative, that they have plausibly alleged a "would not have shopped" theory. (Doc. 48, pp. 26–27). In arguing that there is no requirement to itemize the amount paid for data security, Plaintiffs rely on the fact that *In re SuperValu* applied Illinois law. However, Illinois and Arkansas law have very similar standards for pleading unjust enrichment claims. *Compare In re SuperValu*, 925 F.3d at 966 (quoting *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.*, 545 N.E.2d 672, 679 (Ill. 1989) ("a plaintiff must allege that the defendant has unjustly retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience.")), *with Friedman*, 788 F.3d at 866 (quoting *Campbell*, 381 S.W.3d at 36 ("a person must have 'received money or its equivalent under

such circumstances that, in equity and good conscience, he or she ought not to retain.'")). The Court thus finds *In re SuperValu* persuasive notwithstanding the difference in state law.

Plaintiffs also advance the "would not have shopped" theory discussed in *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154 (D. Minn. 2014). "The 'would not have shopped' theory is where a customer would not have purchased the good or service had they been fully informed about it, and, thus, the merchant is not entitled to the money it received." *In re Brinker*, 2020 WL 691848, at *10. Plaintiffs advance a version of that theory, alleging "[i]f Plaintiffs and Class Members knew that Mena had not secured their Private Information, they would not have agreed to provide their Private Information to Mena." (Doc. 45, ¶ 242).

The Court does not find *In re Target* persuasive for the same reason the *In re Brinker* court rejected the "would not have shopped" theory. The *In re Brinker* court rejected that theory because "unlike *Target*, Plaintiffs never allege Brinker knew about the breach at the time Plaintiffs were dining at [Defendant's restaurant]." 2020 WL 691848, at *11. That court goes on to say "*Target* appears to be an outlier among data breach cases in recognizing the 'would not have shopped' theory, which is likely attributable to the unique circumstance that Target allegedly knew about the breach as it was ongoing." *Id.* (citation omitted). The same reasoning applies here. Plaintiffs have not adequately alleged that Mena knew of the data breach and withheld that information from Plaintiffs before they were patients. Instead, Plaintiffs simply allege that they would not have gone to Mena for medical services if they knew Mena had not secured their PII. This Court will not extend the "would not have shopped" theory so far.

The Eighth Circuit has previously made clear that unjust enrichment claims have not been plausibly alleged when plaintiffs fail to allege plaintiffs "a benefit conferred in exchange for protection of [their] personal information." *In re SuperValu*, 925 F.3d at 966. Moreover, the

"would not have shopped" theory does not apply to the Plaintiffs' allegations here. Therefore, the Court will dismiss Plaintiffs' claim for unjust enrichment.

E. Invasion of Privacy

Plaintiffs allege Mena invaded their privacy. Arkansas law recognizes four distinct invasion of privacy claims: (1) intrusion upon seclusion, (2) appropriation of another's name or likeness, (3) public disclosure of private facts, and (4) false light. *Dodrill v. Ark. Democrat Co.*, 590 S.W.2d 840, 844 (Ark. 1979). Plaintiffs do not identify which type of claim they pursue in their complaint, but Plaintiffs' response to the motion to dismiss only cites caselaw related to the public disclosure of private facts. Therefore, the Court will evaluate the invasion of privacy claim under the public disclosure of private facts theory.

The elements of a public disclosure of private facts claim are: "(1) that [plaintiff] sustained damages; (2) that [defendant] made a public disclosure of a fact about [plaintiff]; (3) that prior to disclosure the fact was not known to the public; (4) that a reasonable person would find the disclosure highly offensive; (5) that [defendant] knew or should have known that the disclosed fact was private; (6) that the fact was not of legitimate public concern; and (7) that the public disclosure was the proximate cause of the plaintiff's damages." *Dillard v. City of Springdale*, 2022 WL 403287, at *7 (W.D. Ark. Feb. 9, 2022) (citing *Duggar v. City of Springdale*, 599 S.W.3d 672, 685 (Ark. Ct. App. 2020)). These elements are taken from Arkansas Model Jury Instruction 422. *Id.*

Plaintiffs allege that "Mena failed to protect and released to unknown and unauthorized third parties" Plaintiffs' PII. (Doc. 45, ¶ 250). As to Mena's state of mind, Plaintiffs allege "Mena acted with a knowing and intentional state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient." *Id.* ¶ 255. The Plaintiffs further allege "[b]ecause Mena acted with this knowing

state of mind, it had notice and knew the inadequate and insufficient security practices would cause injury and harm to Plaintiffs and the Class." *Id.* ¶ 256.

Plaintiffs have not adequately pleaded how Mena "made a public disclosure." At the outset of their complaint, Plaintiffs allege Mena "lost control over its computer network and its patients' highly sensitive information in a data breach perpetrated by cybercriminals. . . ." (Doc. 45, ¶ 1). Plaintiffs also allege "Mena's internal investigation revealed that an unauthorized third party had accessed and removed a number of files from Mena's system over a year ago in the Data Breach." *Id.* ¶ 2. Plaintiffs' tone shifts in the section on their invasion of privacy claim, with Mena now allegedly "releasing to unknown and unauthorized third parties" Plaintiffs' PII." *Id.* ¶ 250. True, Plaintiffs can set out inconsistent claims. Fed. R. Civ. P. 8(d)(3). But Plaintiffs' claims must contain more than mere labels, conclusions, or the elements of their claims. *Bell Atl. Corp.*, 550 U.S. at 555. The Court finds Plaintiffs' invasion of privacy claim does not meet this standard.

The Court's decision is supported by other district courts who have rejected invasion of privacy claims in the data breach context. Courts are split about whether invasion of privacy claims can survive a motion to dismiss in the data breach context. *Compare In re Ambry Genetics*, 567 F. Supp. 3d at 1143 (denying motion to dismiss under California law), *with Purvis v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360, 1377 (N.D. Ga. 2021) (granting motion to dismiss under Georgia law). The Court is persuaded by the *Purvis* court, which explained "Plaintiffs have not plausibly alleged any facts indicating that Defendant—as opposed to the third party that allegedly carried out the Data Breach—actively participated in the alleged intrusion into Plaintiffs' affairs." 563 F. Supp. 3d at 1377.

The same reasoning applies here. Plaintiffs have not alleged any facts that Mena intentionally disclosed Plaintiffs' PII rather than the PII being removed by the third parties.

Plaintiffs conclude that Mena released the information, but do not support that conclusion with any facts. Plaintiffs allege Mena acted intentionally because it "permitted the Data Breach to occur" because of its knowledge of its inadequate data practices. (Doc. 45, ¶ 255). The allegation that Mena had inadequate data practices is better presented in Plaintiffs' negligence claim, which survives the motion to dismiss. *Cf. Farmer*, 582 F. Supp. 3d at 1188 ("Farmer's invasion-of-privacy claim fails because he does not allege that Humana or Cotiviti intentionally disclosed his PII and PHI to unauthorized persons. Instead, Farmer pleads that Defendants' negligent 'failure to protect the PII and PHI' resulted in the disclosure.").

In sum, Plaintiffs' invasion of privacy claim alleges only mere labels or conclusions which are unsupported by factual allegations. Plaintiffs have not alleged how Mena—as opposed to the third-party cybercriminals—intentionally disclosed Plaintiffs' PII. Therefore, the Court will dismiss Plaintiffs' claim for invasion of privacy.

F. Stored Communications Act

Plaintiffs' last claim is that Mena violated the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2713. The SCA creates a civil cause of action for "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind. . . ." 18 U.S.C. § 2707(a). The Eighth Circuit has recognized "[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer networks."). *Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 839 (8th Cir. 2015) (quoting Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004)).

Plaintiffs claim Mena violated two SCA sections. Plaintiffs allege "[b]y failing to take reasonable steps to safeguard Plaintiffs' and Class Members' [PII] while in electronic storage, Mena has allowed unauthorized access to its electronic systems and knowingly divulged [PII]." (Doc. 45, ¶ 272). The two SCA sections Plaintiffs rely on contain terms of art, so the Court believes it is better to reproduce the sections as a whole:

> **(1)** a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> **(2)** a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> > **(A)** on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service. . . .

18 U.S.C. §§ 2702(a)(1) to (2)(A). The SCA defines both "electronic communication service" and "remote computing service." "'Electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15). "'Remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2).

Mena argues that the SCA claim should be dismissed for two reasons. First, Mena argues it is neither an electronic communication service nor a remote computing service. Second, Mena argues that Plaintiffs have not alleged facts showing Mena knowingly divulged their PII. Plaintiffs oppose both arguments. The Court agrees with Mena.

First, the Court has serious doubts that Mena provides either an electronic communication service or a remote commuting service. *See Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("Courts have concluded that 'electronic communication service'

encompasses internet service providers as well as telecommunications companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online[.]"). Plaintiffs conclude that Mena provides an electronic communication service to the public. (Doc. 45, ¶ 271). But Plaintiffs do not allege how Mena provides users the ability to send or receive wire or electronic communications. Conclusions are not enough to state a claim. *Bell Atlantic Corp.*, 550 U.S. at 555. Plaintiffs allege that "Mena stores its patients' [PII] and utilizes such information to provide services to its patients." (Doc. 45, ¶ 276). But again, this does not allege how Mena has provided users either "the ability to send or receive wire or electronic communications" (18 U.S.C. § 2510(15)) or show that Mena provides "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).[12]

Second, assuming without deciding that Mena is either an electronic communication or a remote computing service under the SCA, Plaintiffs have not alleged facts sufficient to show Mena knowingly divulged their PII. The SCA does not define "knowingly," and the parties agree that the Eighth Circuit has not defined what "knowingly divulge" means under section 2702. The Court does not face a blank slate, however, as courts in other circuits have defined "knowingly." Most persuasively, the Sixth Circuit addressed the definition of "knowingly" in *Long v. Insight*

[12] The Court is also unsure the Plaintiffs' PII qualifies as "contents of a communication" under the SCA 18 U.S.C. § 2702(a). The SCA prohibits knowingly divulging "contents of a communication." *Id.* The SCA does not definite communication but defines contents as "when used with respect to any wire, oral, or electronic communication, includ[ing] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). The parties did not brief this issue and it is not dispositive, so the Court has assumed without deciding that the Plaintiffs' PII is covered by the SCA. The Court doubts that assumption would hold up to closer scrutiny had the parties briefed the issue.

Commc'ns of Cent. Ohio, LLC, 804 F.3d 791 (6th Cir. 2015). The *Long* court held that a plaintiff cannot state an SCA claim by alleging the defendant "negligently or recklessly fail[ed] to establish the accuracy of the information it disclosed in response to the subpoena." *Id.* at 796. In doing so, the *Long* court cited the legislative history of section 2702(a), where Congress explained: "The requirement that a violator must 'knowingly' divulge the contents is intended to make clear that 'reckless' or 'negligent' conduct is not sufficient to constitute a violation of this section." *Id.* at 797–98 (*first quoting* S. Rep. 99–541, at 36–37, *then citing* H. Rep. 99–647, at 64 ("The concept of 'knowingly' does not include, however, 'reckless' or 'negligent' conduct.")). The Court agrees that the most natural reading of the phrase "knowingly divulge" requires more than alleging negligent or even reckless conduct.

Here, Plaintiffs allege Mena "fail[ed] to take reasonable steps to safeguard Plaintiffs'" PII. (Doc. 45, ¶ 272). At least one district court has held nearly identical language does not state a claim under the SCA. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017) ("Plaintiffs allege only that Defendants 'fail[ed] to take commercially reasonable steps' to safeguard' [sic] Plaintiffs' communications. This allegation, without more, does not establish that Defendants 'divulge[d]' Plaintiffs' PII and did so with a knowing state of mind."). Just as with the invasion of privacy claim, the Court finds Plaintiffs have not alleged any facts demonstrating that Mena intentionally or knowingly disclosed Plaintiffs' PII rather than the PII being removed by the third parties.

Plaintiffs' response to the motion to dismiss focuses on the allegations that Mena's system lacked required security measures, that Mena should have known healthcare providers are common targets, and that Mena failed to create reasonable safeguards for the PII. *See* Doc. 48, p. 34. But again, nothing in those allegations shows that Mena itself knowingly divulged the Plaintiffs'

information. *Cf. Pica v. Delta Air Lines, Inc.*, 2019 WL 1598761, at *9 (C.D. Cal. Feb. 14, 2019), *aff'd,* 812 F. App'x 591 (9th Cir. 2020); *see also Willingham v. Global Payments, Inc.*, 2013 WL 440702, at *12 (N.D. Ga. Feb. 5, 2013) ("Plaintiffs have not alleged any act by Defendant Global Payments, only that Defendant, which was PCI DSS compliant at the time, somehow created or contributed to the breach of its data system."). To be sure, Plaintiffs have alleged that Mena's faulty systems may have contributed to the data breach, but that is not the same as alleging Mena knowingly divulged the PII.

The SCA is not a sweeping catch-all protection for stored internet communications. *Anzaldua*, 793 F.3d at 839. Even assuming the SCA applies to Mena, Plaintiffs have not alleged that Mena "knowingly divulge[d]" their PII. For that reason, the Court will dismiss Plaintiffs' SCA claim.

G. Declaratory Judgment

Finally, Mena argues the declaratory judgment claim should be dismissed because it is not a standalone cause of action but a type of remedy. (Doc. 47, p. 25). Plaintiffs agree that declaratory judgment is not an independent cause of action but argue they can pursue declaratory relief to the extent their substantive claims survive. (Doc. 48, p. 29). The Court agrees with the parties that any declaratory relief depends on Plaintiffs' substantive claims surviving the motion to dismiss. *See Pub. Water Supply Dist. No. 10 of Cass Cnty. v. City of Peculiar*, 345 F.3d 570, 572 (8th Cir. 2003) ("The Declaratory Judgment Act did not extend federal court jurisdiction beyond the recognized boundaries of justiciability, but only 'enlarged the range of remedies available.'") (quotation omitted); *see also N. Bottling Co. v. Henry's Foods, Inc.*, 474 F. Supp. 3d 1016, 1029 (D.N.D. 2020) (dismissing declaratory judgment claim "[b]ecause [plaintiff] has not adequately

alleged an underlying claim"). Because the Court has not dismissed all of Plaintiffs' substantive claims, the Court will not dismiss the declaratory judgment claim.

IV. Conclusion

IT IS THEREFORE ORDERED that Mena's motion to dismiss (Doc. 47) is GRANTED IN PART and DENIED IN PART. The Plaintiffs' breach of fiduciary duty, unjust enrichment, invasion of privacy, and Stored Communications Act claims are DISMISSED WITHOUT PREJUDICE. The Plaintiffs' negligence, implied breach of contract, and declaratory judgment claims remain pending. The Court will separately issue a final scheduling order.

IT IS SO ORDERED this 1st day of November, 2023.

/s/ P. K. Holmes, III

P.K. HOLMES, III
U.S. DISTRICT JUDGE