UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI, WESTERN DIVISION

O.S. and F.C., individually and on behalf of all others similarly situated, et al. v. Mid America Physician Services, LLC

O.S. and F.C. v. Mid America Physician Services · No. 4:25-cv-00685-RK · Decided April 13, 2026

SUMMARY

The United States District Court for the Western District of Missouri considers Mid America Physician Services, LLC's Rule 12(b)(6) motion to dismiss a putative class action arising from a November 2024 data breach. The court grants the motion in part, dismissing without prejudice claims for negligence, negligence per se, invasion of privacy, breach of fiduciary duty, and violation of the Missouri Merchandising Practices Act. Claims for breach of implied contract, unjust enrichment, and declaratory and injunctive relief remain.

OPINION

O.S. AND F.C., O.S. AND F.C., INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, et al. v. MID AMERICA PHYSICIAN SERVICES, LLC
PER CURIAM.
IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION
O.S. AND F.C., O.S. AND F.C.,)
INDIVIDUALLY AND ON BEHALF OF)
ALL OTHERS SIMILARLY SITUATED,;)
et al.,)) Case No. 4:25-cv-00685-RK Plaintiffs,)) v.))
MID AMERICA PHYSICIAN SERVICES,)
LLC,)
) Defendant.)
ORDER
This is a putative class action against Mid America Physician Services, LLC ("MAPS"), following a data breach on or about November 14, 2024. Before the Court is Defendant MAPS's motion to dismiss Plaintiffs' Second Amended Complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure for failure to state a claim. (Doc. 41.) The motion is fully briefed. (Docs. 42, 49, 50.) After careful consideration and review, and for the reasons explained below, the Court ORDERS that the motion to dismiss is GRANTED in part and DENIED in part. The following claims are DISMISSED without prejudice for failure to state a claim: Count 1 (negligence), Count 2

(negligence per se), Count 5 (invasion of privacy), Count 6 (breach of fiduciary duty), and Count 7 (violation of the Missouri Merchandising Practices Act). Accordingly, the claims that remain are: Count 3 (breach of implied contract), Count 4 (unjust enrichment), and Count 8 (declaratory and injunctive relief). Background Mid America Physician Services or MAPS is a Kansas-based medical provider that provides obstetrics and gynecological medical services to women through several facilities located in the state of Kansas surrounding the Kansas City metro area. (Doc. 23-1 at ¶¶ 38, 39.)1 MAPS 1 On October 23, 2025, the Court granted Plaintiffs' unopposed motion to file a second amended complaint and directed Plaintiffs to file the second amended complaint attached to their motion to amend on or before October 30, 2025. (Doc. 27.) Plaintiffs did not do so. For ease of reference and for present purposes, the Court—like MAPS—will cite to the second amended complaint as attached to Plaintiffs' serves patients who are from both Kansas and Missouri. (Id. at ¶ 2.) The named plaintiffs in this putative class action include both Kansans and Missourians who are current and former patients of MAPS. (See id. at ¶¶ 22-33.) Plaintiffs allege that "[t]o receive medical services," they were each "required to provide her Private Information to MAPS, which was then stored on MAPS's computer systems and networks," including their name, address, Social Security numbers, financial information (such as account numbers or credit/debit card numbers), medical information, and health insurance information. (Id. at ¶¶ 47, 168, 183, 198, 213, 228, 243, 258, 273, 288, 303.) On or about November 14, 2024, MAPS discovered a "network incident that impacted its IT systems"; a data breach. (Id. at ¶ 4.) MAPS's investigation of the data breach concluded in early May 2025. Approximately two months later in July 2025, MAPS notified victims that their personal information had been exposed in the breach by posting a notice on its website as well as sending letters to individuals whose private information had been exposed in the breach. (Id. at ¶¶ 5, 6, 46, 49.) Plaintiffs allege that they have been damaged as a result of the data breach and are "placed at an imminent and continuing risk of harm from fraud and identify theft." (Id. at ¶ 83.) They allege that they now must carefully monitor their accounts and any financial activity. (Id.) They allege harm including actual identify theft, potential fraud and identify theft, loss of privacy, out- of-pocket expenses and value of time to remedy and mitigate the effects of the data breach, and damage to their credit, among other harms. (Id. at ¶ 85.) Plaintiffs allege that "the Data Breach was a direct result of MAPS's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect" the private information they gave to MAPS in order to receive medical care and that, as a healthcare provider in particular, MAPS knew or should have known of the risks and harm of a data breach. (Id. at ¶¶ 8, 98, 99.) Plaintiffs assert eight claims in this putative class action: Count 1 (negligence), Count 2 (negligence per se), Count 3 (breach of implied contract), Count 4 (unjust enrichment), Count 5 (invasion of privacy), Count 6 (breach of fiduciary duty), Count 7 (violation of the Missouri Merchandising Practices Act), and Count 8 (declaratory and injunctive relief). (Id. at 74-99.) motion to amend at Doc. 23-1 as the operative complaint. Legal Standard To survive a motion to dismiss pursuant to rule 12(b)(6) of the Federal Rules of Civil Procedure, "a complaint

must contain sufficient factual matter, accepted as true, to 'state a claim for relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). "A claim is facially plausible where the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Wilson v. Ark. Dep't of Hum. Servs., 850 F.3d 368, 371 (8th Cir. 2017) (internal quotation marks omitted). While a complaint does not need to include detailed factual allegations, the complaint must allege more than a sheer possibility that a defendant acted unlawfully to survive a motion to dismiss. Id. (citation omitted). Discussion I. Count 1 – Negligence (Duty to Protect Against Breach) In Count 1, Plaintiffs assert a claim for ordinary negligence under Missouri law.2 To state a claim for negligence, Plaintiffs must allege facts plausibly showing: "(1) the existence of a legal duty owed to the plaintiff, (2) breach of that duty through a negligent act by the defendant,

(3) proximate causation between the breach and the resulting injury, and (4) resulting damages." Ostrander v. O'Banion, 152 S.W.3d 333, 338 (Mo. banc 2004). MAPS argues that Plaintiffs fail to adequately plead elements (1) legal duty and (2) breach. When, as here, a federal court sits in diversity jurisdiction (including under the Class Action Fairness Act or 28 U.S.C. § 1332(d)) it determines substantive state law by looking to decisions by the state's supreme court, or in the absence of such precedent, by relying on other sources including "relevant state precedent, analogous decisions, considered dicta and any other reliable data" to "predict how [the state supreme court] would decide the issue." Olmsted Med. Ctr. v. Continental Cas. Co., 65 F.4th 1005, 1008 (8th Cir. 2023) (internal quotation marks omitted; quotation modified). Under Missouri common law, "whether a duty exists in a particular case" depends on "the foreseeability of the injury, the likelihood of the injury, the magnitude of the burden of guarding against it and the consequences of placing that burden on defendant." Hoffman v. Union Elec. Co., 176 S.W.3d 706, 708 (Mo. banc 2005). "The touchstone for the creation of a duty is 2 The parties both apply Missouri law to each of Plaintiffs' claims, so the Court does as well. foreseeability." L.A.C. ex rel. D.C. v. Ward Parkway Shopping Ctr. Co., LP, 75 S.W.3d 247, 257 (Mo. banc 2002) (internal quotation marks omitted). Accordingly, as a general rule under Missouri law, there is no "duty to protect against the criminal acts of third parties . . . because such activities are rarely foreseeable." Id.; accord Meadows v. Friedman R.R. Salvage Warehouse, Div. of Friedman Bros. Furniture Co., 655 S.W.2d 718, 720 (Mo. Ct. App. 1983) ("There exists no general duty to protect a plaintiff against the intentional criminal conduct of unknown third persons."). In L.A.C., however, the Missouri Supreme Court recognized that "in situations where a special relationship exists, such as that between a business owner and invitee, and injury is foreseeable to recognizable third parties, a duty will be imposed" even for criminal acts of third parties. 75 S.W.3d at 257. The state supreme court thus held that "a duty to exercise care to protect business invitees may be imposed by common law under the facts and circumstances of a given case." Id. (quoting Madden, 758 S.W.2d at 62 (quotation modified)). In Wieland v. Owner- Operator Services, Inc., 540 S.W.3d

845 (Mo. banc 2018), the Missouri Supreme Court explained that it had recognized in L.A.C. "two 'special facts and circumstances' exceptions to the rule that businesses generally have no duty to protect invitees from criminal acts of third persons," as follows: Under the first exception, the duty [of care] may arise when a person, known to be violent, is present on the premises or an individual is present who has conducted himself so as to indicate danger and sufficient time exists to prevent injury. Because the first exception concerns when a business knows or has reason to know a specific third person is both (1) on its premises and (2) dangerous, no duty of care arises until after that specific person has entered the business's premises. In contrast, the second exception recognizes a duty on the part of business owners to protect their invitees from the criminal attacks of unknown third persons under certain special circumstances. Because the second exception concerns when a business knows or has reason to know of dangerous persons in general frequenting its premises, a duty of care arises without regard to any specific person entering the business's premises. In other words, with the second exception, the business is tasked with taking precautionary actions to protect its business invitees against the criminal activities of unknown third parties. Id. at 849 (internal quotation marks omitted; citations omitted; quotation modified).3 3 Missouri law also recognizes certain "special relationships" that by virtue of the relationship alone gives rise to a duty to protect a party against criminal conduct by unknown third persons: "innkeeper-guest, common carrier-passenger, school-student, and sometimes employer-employee." R.C. v. Sw. Bell Tel. Co., 759 S.W.2d 617, 620-21 (Mo. Ct. App. 1988). As the Missouri Court of Appeals explained in R.C., however, the kinds of "special relationships" that give rise to a duty to protect from the criminal acts by unknown third parties "are concerned with providing a physical place of safety." Id. Missouri courts have Plaintiffs' theory of MAPS's duty of care here in this data-breach context is that "entities that choose to collect or retain sensitive personal data may owe a duty of reasonable care to safeguard that information." (Doc. 49 at 8.) Plaintiffs cite no caselaw from Missouri state courts recognizing a duty of care arising from the broadly stated relationship, i.e., entity which collects sensitive personal data and customer/consumer/individual who provides sensitive personal data to that entity. The Seventh Circuit examined both Illinois and Missouri law to determine whether a common law duty to protect customer data exists in the data breach context in Community Bank of Trenton v. Schnuck Markets, Inc., 887 F.3d 803 (7th Cir. 2018). In that case, as relevant here, a customer brought a negligence claim against a grocery store chain following a data breach. Acknowledging the lack of guidance by Missouri's appellate courts as to the existence of an applicable "duty" as to the customer's negligence claim, the Seventh Circuit considered Missouri's data privacy statute, § 407.1500, RSMo, "whose only consumer-facing mandate is notice," and the fact that Missouri's Attorney General has exclusive authority to enforce the data-breach-notice statute by civil action. Id. at 818. The Seventh Circuit concluded that Missouri courts would not recognize a common law duty to safeguard customer/client data. Id.4 not expanded this exception further than these identified limited relationships. Nor do Plaintiffs' claims here implicate physical safety. Cf.

Bradley v. Ray, 904 S.W.2d 302, 311 (Mo. Ct. App. 1995) (holding that the psychiatrist-patient relationship itself imposes as a matter of Missouri common law a duty to warn identifiable victims of the violent intentions of a patient). Accordingly, the Court considers whether Plaintiffs sufficiently allege a duty to protect or secure their private information under the framework set out by the Missouri Supreme Court in L.A.C. 4 As to the negligence claim arising under Illinois law, the Seventh Circuit principally relied on an Illinois Court of Appeals opinion in Cooney v. Chicago Public Schools, 943 N.E.2d 23 (Ill. App. Ct. 2010), in which the state court of appeals found no common law duty to safeguard information or data similarly considering that Illinois' data privacy law imposed no duty beyond providing notice of a security breach. See Cmty. Bank of Trenton, 887 F.3d at 816 (discussing Cooney). Following Cooney (and the Seventh Circuit's decision in Community Bank of Trenton), the Illinois legislature amended the state's data privacy law "to require data collectors in possession of the personal information of Illinois residents to 'implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.'" Flores v. Aon Corp., 242 N.E.3d 340, 353 (Ill. App. Ct. 2023) (quoting Pub. Act. 99-503 (eff. Jan. 1, 2017) (adding 815 ILCS 530/45)). Accordingly, in Flores, the Illinois Court of Appeals held that "[g]iven that the legislature has now created a duty to maintain reasonable security measures under the Information Protection Act, the reasoning of the Cooney court no longer applies." Id. The Illinois Court of Appeals then found a common law duty under Illinois state law to protect personal information of clients or customers. Id. Thus, while Cooney is no longer good law following the state legislature's statutory amendment, its reasoning (and by extension the Seventh Circuit's reasoning in Community Bank of Trenton) as to The Court is persuaded by the Seventh Circuit's analysis. Although the Eighth Circuit has not yet had occasion to weigh in on this issue of Missouri substantive law, the Court of Appeals did adopt the Seventh Circuit's analysis of Illinois law based on Cooney, (see note 4, above), which considered the scope and nature of Illinois' data-privacy statute which, at that time, was substantially similar to Missouri's data breach statute. In re SuperValu, Inc., 925 F.3d 955, 963 (8th Cir. 2019). The Eastern District has similarly recognized that Missouri courts do not appear to have adopted a "general, common law duty to safeguard information from criminal cyberattack." Mackey v. Belden, Inc., No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *6 (E.D. Mo. Aug. 3, 2021); see Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1055 (E.D. Mo. Nov. 23, 2009) (predicting that Missouri common law does not recognize a duty to provide adequate and timely notice of a data breach considering the limited scope of Missouri's data privacy statute). Missouri courts, including the Missouri Supreme Court, have recognized, however, that physicians have a "fiduciary duty of confidentiality not to disclose any medical information received in connection with his treatment of the patient." Howland v. Truman Med. Ctr., Inc., 719 S.W.3d 98, 107 (Mo. Ct. App. 2025) (quoting Brandt v. Med Def. Assocs., 856 S.W.2d 667, 670 (Mo. banc 1993)). Thus, given the nature of this special relationship identified by Missouri courts particularly in regards to patient information, the Court considers

whether, as a matter of law, Plaintiffs have alleged sufficient circumstances known to MAPS such that "a reasonable person" would have anticipated the data breach that occurred and would have "take[n] precautionary actions to protect" against it. L.A.C., 75 S.W.3d at 258; see Wieland, 540 S.W.3d at 849 ("[W]hen a business knows or has reason to know of dangerous persons in general frequenting its premises, a duty of care arises without regard to any specific person entering the business's premises."); Hyde v. City of Columbia, 637 S.W.2d 251, 272 (Mo. Ct. App. 1982) ("Our law imposes liability in negligence for an intentional injury where the original actor creates a condition which he knows or should foresee will give occasion to a third person to commit an intentional injury upon the plaintiff."). Missouri law remains persuasive. Flores even buttresses the analysis in those cases to the extent a different outcome was required in that case based on the particular post-Cooney amendments to Illinois' data privacy law. Missouri's data-privacy law has not similarly been amended. In this regard, Plaintiffs primarily rely on the asserted modern prevalence of cybersecurity attacks and the specific targeting of the healthcare industry by cybercriminals as the basis for why MAPS "should have been aware, and indeed was aware, that it was at risk of" a cyberattack and that it "was aware of the risks and harm that could result from inadequate data security . . . ." (See Doc. 23-1 at ¶¶ 92-99.) In this context, Plaintiffs allege that MAPS had a "duty to implement and maintain reasonable data security practices" and "to provide data security consistent with industry standards and other requirements . . . to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected" Plaintiffs' private information. (Id. at ¶¶ 363, 366.) The Missouri Supreme Court has not yet decided the "precise requirements" of the "special circumstances" exception recognized in L.A.C. See 75 S.W.3d at 258 (declining to "enter the fray" concerning the appropriate test or standard, including a "prior similar incidents" or "totality of the circumstances" approach). Under the "prior similar incidents" standard, a defendant has sufficient notice when the prior incidents are "(1) sufficiently numerous, (2) recent, and (3) similar in type to the prior specific incidents to render further incidents foreseeable." Simmons v. Keat Props., LLC, 717 S.W.3d 259, 266 (Mo. Ct. App. 2025) (internal quotation marks omitted). Under a totality of the circumstances approach, "the factors to be considered include the nature of the business location, the character of the business, and past events in the area." Id. at 268 (internal quotation marks omitted). Under any approach, the Court should "only consider[] those incidents on the premises and in the area." Id. at 268; see Faheen ex rel. Hebron v. City Parking Corp., 734 S.W.2d 270, 273-74 (Mo. Ct. App. 1987) ("[T]here must be prior specific incidents of violent crimes on the premises that are sufficiently numerous and recent to put a defendant on notice, either actual or constructive, that there is a likelihood third persons will endanger the safety of defendant's invitees.") (referring to "[t]he basic requirements" of duty under these circumstances as "notice, specificity, and probability of harm to the victim"). The Eighth Circuit, in the premises liability context and applying Missouri law in particular, has similarly cautioned against "expand[ing] the relevant premises too far": "[f]or off- premises crimes to be relevant, there must be a discernable link to the premises." Aaron

v. Nat'l R.R. Pass. Corp., 163 F.4th 503, 510 (8th Cir. 2025); see Liszewski v. Target Corp., 374 F.3d 597, 599 (8th Cir. 2004) ("[A]n offense is reasonably foreseeable and a duty arises under circumstances where prior reports of criminal activity or other similar acts on or near the site are sufficient in number, sufficiently similar to, and sufficiently close in time to the immediate offense to place a business on notice of the need to protect its invitees from that general type of risk."). "[N]ationwide incidents" do not alone provide sufficient notice to establish foreseeability giving rise to a common law duty to protect as an exception to the general rule that no duty is owed to protect another from the criminal acts of third parties. Simmons, 717 S.W.3d at 269. The Court is cognizant that "[b]efore extending a legal duty to a novel set of facts, [it] must exercise caution." Colley v. Neighbors Credit Union, No. 4:25-CV-00687-SRC, 2026 WL 864583, at *13 (E.D. Mo. Mar. 30, 2026). For "[i]t is not the role of a federal court [sitting in diversity] to expand state law in ways not foreshadowed by state precedent." Ashley County v. Pfizer, Inc., 552 F.3d 659, 673 (8th Cir. 2009). The Court is persuaded that the Missouri Supreme Court would not recognize a general or "data privacy" duty of care for the reasons explained by the Seventh Circuit in Community Bank of Trenton (as adopted by the Eighth Circuit in In re SuperValu, at least as to Illinois law). To be sure, MAPS collected and retained Plaintiffs' private information (medical, personal, and financial) in the course of providing medical care to Plaintiffs and had a fiduciary duty of confidentiality not to disclose Plaintiffs' private medical information. As explained in § VI below, however, this fiduciary duty is somewhat narrow in its scope and nature. It is implicated only when the physician or medical provider actively discloses a patient's private medical information. Furthermore, Missouri's data privacy law explicitly refers to both personal information (such as name, social security number, etc.), as well as health insurance information and even medical information. See Mo. Rev. Stat. § 407.1500.1. Although it is somewhat imperfect as an analogue, the premises-liability caselaw referenced above is helpful to predict what the Missouri Supreme Court would do in this data breach context, which similarly considers precautionary protection against intentional criminal acts of third persons causing the alleged personal harm. Under L.A.C.'s "relationship plus" formulation of a legal duty framework, something more than a generalized and conceivable threat environment is required to give rise to an actionable duty to impose liability in tort. See Irby v. St. Louis Cty. Cab Co., 560 S.W.2d 392, 395 (Mo. Ct. App. 1977) ("The allegation of a 'high crime area' does not ipso facto mandate" a duty to protect against intentional criminal acts of third parties.) In L.A.C. itself, for example, the Missouri Supreme Court held that (1) incident reports of prior violent crimes occurring on mall property and (2) testimony by the corporate security director for the mall management services provider who acknowledged that "rape in isolated areas of a mall is security concern" and is a "crime that we are constantly vigilant for" supported, as a legal proposition, that "[c]ontinued violent crime, such as the alleged rape of L.A.C. was foreseeable." 75 S.W.3d at 259. Thus, the Missouri Supreme Court held, the mall "had a duty to take reasonable measures to protect mall customers . . . from this type of violent criminal activity." Id. In In re Equifax, Inc., Customer Data

Sec'y Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019), a data breach case, the district court found (applying Georgia law) that the plaintiffs plausibly stated that the defendant, Equifax, owed a duty of care to safeguard information in its custody where they alleged that Equifax "knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures" where "Equifax recognized the importance of data security"; had "observed other major, well-publicized data breaches," including a data breach of its competitor Experian; that it "held itself out as a leader in confronting such threats" and had "acquired two identity theft protection companies"; and that it had itself "suffered several different data breaches incidents highlighting deficiencies in its cybersecurity protocol." Although not a data breach case, the district court in Rardon v. Falon Safety Prods., Inc., No. 20-6165-CV-SJ-BP, 2021 WL 2008923 (W.D. Mo. May 4, 2021), similarly found that a plaintiff alleged sufficient facts to plausibly state a duty of care under Missouri law in asserting a negligence claim against a manufacturer (Falcon Safety Products) and seller (Wal-Mart) of a compressed-air dust cleaner (Dust-Off) after a third party (Shawn Yuille) caused a fatal car accident when he inhaled from a can of Dust-Off while driving to get high and lost consciousness. See id. at *3-5. There, the district court found that "the Complaint contains numerous factual allegations demonstrating [the manufacturer and seller]'s knowledge that Dust-Off is inhaled by people while driving in order to get high, thereby causing a risk of harm to others." Id. at *5. Specifically, the plaintiff had alleged that Falcon Safety Products (the manufacturer) added a bittering agent to its product "to discourage people from inhaling the product" and that Wal-Mart had required Falcon Safety Products "to advertise the existence of a bittering agent on its Dust-Off label in response to known incidents of dust remover abuse." Id. at *1. Plaintiff alleged that "inhaling products with [difluoroethane] has resulted in, among other things, car accidents." Id. Plaintiff further alleged that the Dust-Off cans included "a label warning that inhaling the product could cause a serious health hazard and result in death" and which label warning also included "a link to three websites containing information about the hazards of inhalant abuse." Id. (internal quotation marks omitted; quotation modified). The plaintiff further alleged that "the bittering agent does not work in that it does not deter people from using Dust-Off as an inhalant" in part because it "does not mix" with the propellant (difluoroethane), the addictive component and is not emitted when the product is sprayed. Id. Here, the Court finds that Plaintiffs do not allege any facts plausibly showing that MAPS similarly knew or should have known a cybersecurity attack or data breach by third-party cybercriminals was foreseeable. The generalized threat environment of cyber-hacking or data breaches alone is not sufficient under Missouri law. See Irby v. St. Louis Cnty. Cab Co., 560 S.W.2d 392, 395 (Mo. Ct. App. 1977) ("The allegation of a 'high crime area' does not ipso facto mandate this duty [of care to protect against intentional criminal acts of third parties]."). Plaintiffs have not persuasively shown that Missouri law foreshadows the expansion of the law of negligence in this data breach context for which Plaintiffs advocate. Employing "a data security infrastructure in accordance with industry standards does not completely preclude the possibility of a data breach, and conversely a data breach does not by

itself demonstrate an inadequate data security infrastructure." Feins v. Goldwater Bank NA, No. CV-22-00932-PHX-JJT, 2022 WL 17552440, at *7 (D. Ariz. Dec. 9, 2022). Based on the caselaw discussed above, the Court predicts that the Missouri Supreme Court would not recognize the duty of care advocated by Plaintiffs in this data breach circumstance, even as against a medical services provider. And without something more, the Court finds that Plaintiffs do not allege facts to find a duty under Missouri law as an exception to the general rule that there is no duty to protect from the criminal acts of third persons. MAPS's motion to dismiss Count 1 for failure to state a claim is GRANTED. II. Count 2 – Negligence per se (Under the FTC Act and HIPAA) In Count 2, Plaintiffs assert a claim for negligence per se under Missouri law, alleging that MAPS violated certain provisions of federal law under Section 5 of the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45(a), and the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1301, et seq. The Missouri Court of Appeals has held that violation of HIPAA cannot support a negligence per se claim under Missouri law because HIPAA does not provide for a private cause of action. Howland v. Truman Med. Ctr., Inc., 719 S.W.3d 98, 109-110 (Mo. Ct. App. 2025); see Vilcek v. Uber USA, LLC, 902 F.3d 815, 819-20 (8th Cir. 2018) ("Missouri does not allow private cause of action for damages based solely on the violations of a statute unless the legislature intended the violations to be privately actionable.")5 Applying the same logic, because Section 5 of the FTC Act does not provide a private right of action, In re SuperValu, Inc., 925 F.3d 955, 963 (8th Cir. 2019), neither can an alleged violation of Section 5 of the FTC Act support a claim for negligence per se under Missouri law. See Colley, 2026 WL 864583, at *13 (dismissing a claim for negligence per se under Missouri law for failure to state a claim premised on an alleged violation of Section 5 of the FTC Act). MAPS's motion to dismiss Count 2 for failure to state a claim is GRANTED. III. Count 3 – Breach of Implied Contract In Count 3, Plaintiffs assert a claim for breach of implied contract. Under Missouri law, "[t]here is no difference in legal effect between an express contract and one implied in fact."6 Nickel v. Stephens Coll., 480 S.W.3d 390, 397 n.6 (Mo. Ct. App. 2015) (internal quotation marks omitted). MAPS argues that Plaintiffs fail to state a plausible claim for breach of implied contract because they do not sufficiently allege a meeting of the minds or breach. A. Meeting of the Minds An implied contract, like an express contract, "clearly requires a 'meeting of the minds on essential terms.'" Mackey, 2021 WL 3363174, at *8 (quoting Nickel, 480 S.W.3d at 397 n.6). In the context here, "there must have been a meeting of the minds as to [MAPS]'s obligation to reasonably safeguard and protect the [personal information] in order for a breach to have 5 The Missouri Court of Appeals, Western District, in Howland recognized that in J.J. ex rel. C.W. v. Poplar Bluff Regional Medical Center, LLC, 675 S.W.3d 259 (Mo. Ct. App. 2023), the Missouri Court of Appeals, Eastern District, had suggested that a violation of duties under HIPAA might support a claim for negligence per se although at the same time the Eastern District in Poplar Bluff "acknowledged HIPAA does not create a private right of action." Howland, 719 S.W.3d at 110 n.11 (discussing Poplar Bluff). The Missouri Supreme Court has held that "[t]he southern, western and eastern districts of the court of

appeals . . . are not separate courts but simply different districts of a unitary court of appeals." Akins v. Dir. of Rev., 303 S.W.3d 563, 567 n.4 (Mo. banc 2010). Howland, rather than Poplar Bluff, is the better authority of state law on this issue. Not only is Howland directly on point but it also emphasized that the statement in Poplar Bluff indicating that a violation of HIPAA might support a claim for negligence per se under Missouri law was dicta. 6 Missouri courts do recognize "two types of implied contracts: contracts that are implied in law [an equitable claim] and contracts that are implied in fact [not an equitable claim]." Howland, 719 S.W.3d at 108. It is evident that Plaintiffs' claim for breach of implied contract asserted in Count 3 is the latter, to the extent the claim is premised on the allegation that "Defendant's obligation to protect the confidentiality of Plaintiffs' data was an inherent, essential, and non-negotiable term, implied by the very nature of the physician-patient relationship." (Doc. 49 at 13.) occurred." Id. The Court is persuaded that Plaintiffs have plausibly alleged mutual assent or meeting-of-the-minds to survive a motion to dismiss. Plaintiffs allege, at a minimum, that MAPS received their confidential and personal information in the course of providing medical treatment services (and indeed they were required to provide this information to receive medical treatment offered by MAPS); that in addition to its legal and fiduciary duties MAPS "maintained privacy policies governing the" private and sensitive information it collected from patients; and that they would not have provided the private and sensitive information to MAPS absent an implied promise of confidentiality in various respects. See id. Of course, "whether such a contract actually exists is a question of fact" for which Plaintiffs will have the ultimate burden to marshal evidence and meet their burden of persuasion. Suffice it to say, however, that whether an implied contract in fact exists as Plaintiffs allege is "inappropriate for resolution at the motion to dismiss stage." Id. B. Breach MAPS also argues that Plaintiffs fail to plead any breach, principally relying on Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017). Kuhns was a data breach case grounded in a breach of contract cause of action rather than tort (i.e., negligence or breach of fiduciary duty). See id. at 714. The Eighth Circuit held that Kuhns failed to plausibly state a claim for (express) breach of contract: Both parties agree that the Brokerage Agreement governed the relationship and incorporated the Privacy Statement . . . represent[ing] that, "to protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured filings and buildings." The contract also represented that Scottrade provides Secure Socket Layer encryption. The Consolidated Complaint alleges that Scottrade breached the Brokerage Agreement because it "did not comply with applicable laws and regulations as described herein or otherwise adequately safeguard or protect Plaintiffs' personal data from being accessed and taken. Scottrade did not maintain sufficient security measures and procedures to prevent unauthorized access." These assertions do not plausibly allege a breach of contract. First, representations of conditions Scottrade will maintain are in the nature of contract recitals. . . . [And are no more than] bare assertions that Scottrade's efforts failed to protect customer [personal identifying information]. Second . . . the lengthy

Consolidated Complaint fails to allege a specific breach of the express contract. Plaintiffs do not identify a single "applicable law and regulation" that Scottrade allegedly breached regarding its data security practices. . . . The allegation that "Scottrade did not maintain sufficient security measures and procedures to prevent unauthorized access" does not assert more than the mere possibility of misconduct: it is possible that Scottrade breached the Brokerage Agreement, but we have no idea how. Id. at 717 (quotation modified). As to Kuhns's claim for breach of implied contract, the Eighth Circuit held that the claim "must be dismissed for the same failure to allege plausible claims" in that "we are left to guess how Scottrade failed to take 'industry leading' security measures." Id. at 718. The Court is persuaded that Plaintiffs allege more than what had been alleged in Kuhns. For example, Plaintiffs allege that MAPS could have, but did not, utilized "standard practices like the use of industry standard network segmentation and encryption of all Private Information." (Doc. 23-1 at ¶ 117.) Furthermore, Plaintiffs plausibly allege that MAPS did not dispose of patients' private or confidential information and did not otherwise have "proper record retention and destruction practices." (Id. at ¶ 118.) Plaintiffs allege that MAPS "failed to follow" a number of industry best practices, specifically including "to implement multi-factor authentication." (Id. at ¶ 141.) Plaintiffs' allegations are more specific than in Kuhns and allege "more than the mere possibility of misconduct . . . ." 868 F.3d at 717. Whether Plaintiffs can ultimately prove that MAPS breached any implied contract in a particular way (such as not implementing multi-factor authentication) is a question for another day. MAPS's motion to dismiss Count 3 for failure to state a claim is DENIED. IV. Count 4 – Unjust Enrichment In Count 4, Plaintiffs assert a claim for unjust enrichment. A claim for unjust enrichment under Missouri law requires Plaintiffs to plead three elements: (1) that a benefit was conferred on MAPS, (2) MAPS's "appreciation of the fact of that benefit," and (3) that MAPS's retention of the benefit conferred is inequitable under the circumstances. Hennessey v. Gap, Inc., 86 F.4th 823, 830-31 (8th Cir. 2023.) MAPS argues that Plaintiffs fail to state a claim for unjust enrichment because they do not allege any benefit conferred on MAPS, nor allege that MAPS inequitably retained any benefit. In their response brief, Plaintiffs focus primarily on a "cost-savings" theory of unjust enrichment.7 7 The cases cited by MAPS in support of its motion to dismiss in which federal courts dismissed unjust enrichment claims in the data-breach context primarily focus on unjust enrichment claims premised on the monetary value of the private information itself. See Giasson v. MRA-Mgmt. Ass'n, Inc., 777 F. Supp. 3d 913, 940-41 (E.D. Wisc. 2025) (collecting cases rejecting unjust enrichment claims premised on the theory that "conferral of [private information] can itself constitute a benefit for purposes of unjust enrichment," particularly "where, as here, the plaintiff's allegations as to the alleged benefit are extremely Plaintiffs' "cost-savings" theory of unjust enrichment goes as follows: (1) Plaintiffs conferred a benefit on MAPS by providing their private information to MAPS as a condition of receiving medical services, (2) MAPS appreciated the benefit of receiving Plaintiffs' private information by providing Plaintiffs medical services in exchange for payment, and (3) MAPS "was unjustly enriched by not providing Plaintiffs with the

adequate data security [Plaintiffs] expected to receive in exchange for paying for [MAPS]'s services." (Doc. 49 at 18.) In this regard, Plaintiffs allege that they "paid MAPS a certain sum of money, which was used to fund data security" and that "a portion of the payments made . . . was to be used to provide a reasonable level of data security," but that "MAPS enriched itself by saving costs it reasonably should have expended on data security measures and vendors with adequate data security" by "utilizing cheaper, ineffective security measures and vendors." (Doc. 23-1 at ¶¶ 434, 434, 435, 444, 445.) MAPS did not address this unjust enrichment theory in any of its motion-to-dismiss briefing. Federal courts appear to be somewhat divided as to whether this cost-savings theory, particularly in data breach cases, is sufficient to state a claim for unjust enrichment under various other state laws. See Bracy v. Americold Logistics, LLC, No. 1:23-CV-5743-TWT, 2025 WL 552676, at *7-8 (N.D. Ga. Feb. 19, 2025) (recognizing case law falling on both sides of the question). The Eighth Circuit, for its part, has suggested that this theory may be valid. See In re SuperValu, Inc., 925 F.3d at 966 (holding that a plaintiff did not state a plausible claim for unjust enrichment in the data-breach context where the plaintiff "does not allege that any specific portion of his payment went toward data protection" and therefore "has not alleged a benefit conferred in exchange for protection of his personal information" or "how SuperValu's retention of his payment would be inequitable") (applying Illinois law); Kuhns, 868 F.3d at 718 (holding that Kuhns failed to state a claim for unjust enrichment, in part, because "the Consolidated Complaint does not allege that any specific portion of Kuhns's brokerage service fees went toward data protection" (internal quotation marks omitted)) (applying Missouri law); Carlsen v. GameStop, Inc., 833 F.3d 903, 912 (8th Cir. 2016) (holding that Carlsen failed to state a claim for unjust enrichment because "he does vague"); In re Arthur J. Gallagher Data Breach Litig., 631 F. Supp. 3d 573, 591-92 (N.D. Ill. 2022) (dismissing unjust enrichment claim based on "Defendants retain[ing] the monetary benefit of Plaintiffs' valuable [private information]," and recognizing that "Courts have . . . routinely rejected the proposition that an individual's personal identifying information has an independent monetary value" (internal quotation marks omitted)). Plaintiffs do not address (or attempt to defend) this theory in their motion to dismiss response brief. not allege that any specific portion of his subscriber fee went toward data protection," and thus "alleged neither a benefit conferred in exchange for protection of his [private information], nor has he shown how GameStop's retention of his subscription fee would be inequitable"). The Court declines to dismiss Plaintiffs' unjust enrichment claim at this early pleadings stage. MAPS's motion to dismiss Count 4 for failure to state a claim is DENIED. V. Count 5 – Invasion of Privacy In Count 5, Plaintiffs assert a claim for invasion of privacy under Missouri law. Plaintiffs do not contest MAPS's argument that they fail to state a plausible claim for relief for invasion of privacy but instead indicate that they "agree to dismiss their invasion of privacy claim without prejudice at this time." (Doc. 49 at 5 n.1.) MAPS's motion to dismiss Count 5 for failure to state a claim is GRANTED. VI. Count 6 – Breach of Fiduciary Duty In Count 6, Plaintiffs assert a claim for breach of fiduciary duty. To state a claim for breach of fiduciary duty under Missouri law,

Plaintiffs must plead facts showing "[1] a fiduciary duty existed between it and the defending party, [2] that the defending party breached the duty, and
[3] that the breach caused the proponent to suffer harm." W. Blue Print Co., LLC v. Roberts, 367 S.W.3d 7, 15 (Mo. banc 2012) (internal quotation marks omitted). MAPS argues that Plaintiffs fail to state a plausible claim for relief for breach of fiduciary duty under Missouri law because
(1) Plaintiffs have not alleged a fiduciary relationship, and (2) Plaintiffs have not alleged a breach of a fiduciary duty. As noted above, the Missouri Supreme Court has recognized a fiduciary duty of confidentiality arising from the patient-physician relationship. See Brandt, 856 S.W.2d at 670 (recognizing "a fiduciary duty of confidentiality not to disclose any medical information received in connection with [a physician's] treatment of the patient" and that this "duty arises out a fiduciary relationship that exists between the physician and the patient"). MAPS concedes in its reply that a fiduciary relationship exists under Missouri law regarding the confidentiality of at least Plaintiffs' medical information and instead focuses on whether Plaintiffs sufficiently allege a breach of any fiduciary duty. (Doc. 50 at 12.) Accordingly, the Court focuses on the breach element as well. The Court finds that Plaintiffs fail to state a plausible claim for breach of fiduciary duty because they do not allege "facts that [MAPS] disclosed their Private Information to unauthorized third parties." Clay-Platte Family Medicine, 2025 WL 3143638, at *7; see Brandt, 856 S.W.2d at 670 (recognizing a "fiduciary duty of confidentiality not to disclose").8 Plaintiffs do not cite any compelling Missouri law to the contrary. Plaintiffs cite Howland but read it much too broadly. Plaintiffs suggests that the Missouri Court of Appeals in Howland "held that [Howland] sufficiently pled a claim for breach of fiduciary duty where she alleged she was a patient of the medical facility, and that unauthorized individuals accessed her private health information while it was in the possession of the medical facility." (Doc. 49 at 21.) The "unauthorized individuals" in Howland, however, were not third-party independent criminal actors as here, but were instead other employees of the defendant-hospital itself. 719 S.W.3d at 103. In that context, the Missouri Court of Appeals held that Howland stated a claim for breach of fiduciary duty, in part, having "alleged Truman Medical [i.e., the defendant] disclosed her 'patient' medical information." Id. at 108; see also Fierstein v. DePaul Health Ctr., 949 S.W.2d 90, 92 (Mo. Ct. App. 1997) (holding that plaintiff submitted triable claim for breach of fiduciary duty where her physician released Fierstein's records in relation to a subpoena request where Fierstein did not waive her physician/patient privilege). MAPS's motion to dismiss Count 6 for failure to state a claim is GRANTED. VII. Count 7 – Violation of MMPA In Count 7, Plaintiffs assert a claim for violation of the MMPA. "The MMPA provides a private right of action to any person who sustains ascertainable loss in connection with the purchase or lease of merchandise as a result of certain practices declared unlawful." Kuhns, 868 F.3d at 719. In Kuhns, the Eighth Circuit held, in part, that Kuhns failed to state a claim under the MMPA in that data breach case because "Scottrade did not sell data security services; it put data security measures in place to induce customers to voluntarily transfer their [private information] to Scottrade to obtain its brokerage

services.” Id.; see also Conway v. CitiMortgage, Inc., 438 S.W.3d 410, 414 (Mo. banc 2014) (holding that the MMPA “prohibits the use of the enumerated deceptive practices if there is a relationship between the sale of merchandise and the alleged unlawful action”). Plaintiffs assert that Kuhns is distinguishable. They argue that here, unlike in Kuhns, “the confidentiality and data protection . . . are integral, not ancillary” to the medical services provided by MAPS. (Doc. 49 at 24.) Plaintiffs’ argument is not convincing. Plaintiffs provide no persuasive 8 “Disclose” means “to make known or public,” “to expose to view,” or “to open up.” Merriam- Webster’s Collegiate Dictionary 470 (12th ed. 2025). reason why the private information provided to Scottrade in Kuhns—which, indeed, appears to have involved similar personal information, absent the context-specific medical-related information in this case—was any less “integral” or more “ancillary” to Scottrade’s brokerage services that were purchased in Kuhns than the medical services provided by MAPS here. Cf. Clay-Platte Fam. Med., 2025 WL 3143638, at *7-8 (similarly dismissing data-breach MMPA claim, applying Kuhns). To the contrary, the Missouri Court of Appeals has recognized a medical provider’s “keeping of confidential medical records” as “incidental to providing medical treatment.” Poplar Bluff Med. Ctr., 675 S.W.3d at 267 (holding that Missouri law requiring an affidavit of merit in asserting a claim for medical malpractice did not apply to lawsuit stemming from alleged breach of confidentiality of a patient’s private information). MAPS’s motion to dismiss Count 7 is GRANTED. VIII. Count 8 – Declaratory Judgment and Injunctive Relief Finally, in Count 8, Plaintiffs assert a separate claim seeking declaratory and injunctive relief. Because some of Plaintiffs’ substantive claims remain, as set out above, MAPS’s motion to dismiss Count 8 seeking declaratory judgment and injunctive relief is DENIED. Conclusion Therefore, after careful consideration and review, and for the reasons explained above, the Court ORDERS that the motion to dismiss is GRANTED in part and DENIED in part, and that the following claims are DISMISSED without prejudice for failure to state a claim: Count 1 (negligence), Count 2 (negligence per se), Count 5 (invasion of privacy), Count 6 (breach of fiduciary duty), and Count 7 (violation of the Missouri Merchandising Practices Act). Accordingly, those that remain are: Count 3 (breach of implied contract), Count 4 (unjust enrichment), and Count 8 (declaratory and injunctive relief). IT IS SO ORDERED. s/ Roseann A. Ketchmark

ROSEANN A. KETCHMARK, JUDGE

UNITED STATES DISTRICT COURT

DATED: April 13, 2026