

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI  
EASTERN DIVISION**

ANGEL JOEL GUSMAN NEGRON, et al.,	)	
	)	
Plaintiffs,	)	
	)	Case No. 4:24-CV-00669-JAR
vs.	)	
	)	
ASCENSION HEALTH, et al.,	)	
	)	
Defendants.	)	

**MEMORANDUM AND ORDER**

This matter is before the Court on Defendant’s motion to dismiss Plaintiffs’ claims in this putative class action arising from a healthcare system data breach. For the reasons set forth below, the motion will be granted in part and denied in part.

**BACKGROUND**

Defendant Ascension Health and two affiliated companies<sup>1</sup> (collectively, Ascension) comprise a Missouri-based Catholic non-profit healthcare system of 140 hospitals serving 19 states. Plaintiffs were Ascension patients on May 8, 2024, when its technology network suffered a ransomware attack wherein hackers copied electronic files containing patients’ protected health information (PHI) and personally identifiable information (PII). The next day, Ascension posted a notice to its website disclosing a cybersecurity event and describing its response, involving investigation and remediation with expert third-party assistance.

---

<sup>1</sup> The three related Defendants in this case are Ascension Health, its sister company Ascension Health-IS Inc. d/b/a Ascension Technologies, and their parent company Ascension Health Alliance. Ascension summarily contends that the Alliance and Technologies entities should be dismissed from the complaint. But Plaintiffs plead all allegations as to all Defendants. Their respective roles in the events of this case is a matter properly reserved for discovery. To the extent Ascension’s argument could be construed as a motion to dismiss these defendants, it will be denied.

On May 14, 2024, Plaintiffs filed this putative class action asserting claims of negligence (Count I), negligence per se (Count II), breach of implied covenant of good faith and fair dealing (Count III), and unjust enrichment (Count IV) and seeking various forms of injunctive relief and monetary damages. In October 2024, Plaintiffs filed an amended complaint asserting seven claims on behalf of a nationwide class and 11 state law claims specific to seven state subclasses. The proposed nationwide class consists of:

All United States residents whose Personal Information was compromised in the Data Breach discovered by Ascension in May 2024, including all those individuals who receive notice of the breach.

The seven proposed subclasses consist of residents of Arkansas, Florida, Illinois, Indiana, Michigan, Oklahoma, and Wisconsin, respectively. Plaintiffs assert the following counts:

Nationwide Class

- I. Negligence
- II. Negligence per se
- III. Breach of Express Contract
- IV. Breach of Implied Contract
- V. Unjust Enrichment (in the alternative to breach of implied contract)
- VI. Invasion of Privacy
- VII. Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010

Sub-classes

- VIII. Arkansas Deceptive Trade Practices Act, Ark. Code §§ 4-88-101
- IX. Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201
- X. Illinois Personal Information Protection Act, 815 Il. Comp. Stat. § 530/1
- XI. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Il. Comp. Stat. § 505
- XII. Oklahoma Consumer Protection Act, Okla. Stat. tit. 15 § 751
- XIII. Wisconsin Breach of Confidentiality of Health Records Act, Wis. Stat. § 146.81
- XIV. Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18
- XV. Wisconsin Notice of Unauthorized Acquisition of Personal Information Act, Wis. Stat. § 134.98(2)
- XVI. Michigan Identity Theft Protection Act, Mich. Comp. Laws § 445.72
- XVII. Michigan Consumer Protection Act, Mich. Comp. Laws § 445.903
- XVIII. Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-0.1

### Common Facts

The central facts in the complaint common to all counts can be summarized as follows. In connection with the provision of medical services, Ascension creates and stores patients' medical records containing PHI and PII. The Health Insurance Portability and Accountability Act (HIPAA) requires regulated entities like Ascension to maintain appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and safeguard it from improper disclosure. 45 C.F.R. § 164.530(c). Among HIPAA's extensive standards and implementation specifications, Plaintiffs invoke the following regulations (paraphrased) requiring providers to:

1. Ensure the confidentiality, integrity, and availability of electronic PHI; protect against any reasonably anticipated threats or hazards to the security or integrity of such information or impermissible use thereof; and ensure compliance by its workforce. 45 C.F.R. § 164.306.
2. Implement policies and procedures to prevent, detect, contain, and correct security violations; conduct risk assessments; implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306; and implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 45 C.F.R. § 164.308(a)(1).
3. Implement security awareness and training programs for the workforce, including security reminders and updates, protection from malicious software, log-in monitoring, and password management. 45 C.F.R. § 164.308(a)(5).
4. Implement security incident procedures, including identifying, responding to, and reporting suspected or known security incidents and mitigating the impact. 45 C.F.R. § 164.308(a)(6).
5. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1).

Ascension's HIPAA Notice of Privacy Practices states in pertinent part:

**Our Commitment**

We are committed to maintaining the privacy and confidentiality of your health information. This Notice describes your rights concerning your health information and how we may use and disclose (share) your information.

\* \* \*

**Our Responsibilities**

- We are required by law to maintain the privacy and security of your health information.
- We will notify you if a breach occurs that may have compromised the privacy or security of your identifiable health information.

Additionally, Plaintiffs invoke as industry standards guidance contained in a Federal Trade Commission (FTC) publication titled *Protecting Personal Information: A Guide for Business*.<sup>2</sup> The FTC uses its enforcement powers under the Federal Trade Commission Act (FTCA), 15 U.S.C. § 45, to bring actions against businesses for unfair and deceptive data privacy and security practices. The business guide advises companies to inventory, limit, protect, and/or dispose of personal information, understand network vulnerabilities, and implement adequate security policies. It advises entities to limit the retention of and access to sensitive data, encrypt transmissions, update firewalls and malware programs, use authentication systems, require complex passwords, train employees on IT security, use intrusion detection systems, monitor network activity, and create data breach response plans.

Plaintiffs allege that, at the time of the data breach, Ascension maintained its computer systems without encryption and other essential security measures, inconsistent with the foregoing industry standards. As a result, cybercriminals were able to hack into Ascension servers and

---

<sup>2</sup> [Protecting Personal Information: A Guide for Business | Federal Trade Commission](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited September 23, 2025) [<https://perma.cc/YXF8-4Q9C>].

access patient files, thereby exposing patients to identity fraud. Plaintiffs further plead that Ascension was negligent in failing to maintain adequate security, protect patient information, monitor its IT systems for intrusions, train its employees to avoid phishing, comply with FTC cybersecurity guidelines and HIPAA, and adhere to industry standards. Consequently, Plaintiffs face an imminent and ongoing risk of fraud and identity theft that was well-known and foreseeable.

#### Named Plaintiffs

Thirteen named Plaintiffs allege the following common facts.<sup>3</sup> Each Plaintiff was an Ascension patient at the time of the breach. To obtain treatment, they were required to provide PII/PHI, including name, date of birth, address, and social security number (SSN). Each Plaintiff received a copy of Ascension's Notice of Privacy Practices. As a result of the breach, they must now take precautions to mitigate its impact by monitoring accounts for fraudulent activity and checking credit reports. They must also manage spam calls, text messages, and emails. These actions consume time and cause stress. Had they known of Ascension's inadequate security, they wouldn't have provided their information. They suffered actual injuries in the form of invasion of privacy, theft and lost value of PII/PHI, time lost mitigating the effects, the cost of lifetime credit monitoring, the certain ongoing risk to their PII/PHI, lost benefit of bargain, nominal and statutory damages, and emotional stress.

---

<sup>3</sup> A fourteenth individual, Tiffany Farrand, is named as a Plaintiff for the Wisconsin subclass and in corresponding Counts XIII-XV, but there is no mention of her in the Factual Allegations section of the complaint. As such, Ms. Farrand's claims will be dismissed. The Wisconsin subclass remains represented by another named Plaintiff, Jill Radley.

Additionally, eleven of the thirteen named Plaintiffs allege the following individual injuries from the breach.

1. Alma Croft of Alabama was notified by her credit monitoring service that her PII/PHI was disseminated on the dark web. Doc. 52 ¶ 103.

2. Vikesha Exford of Alabama has incurred fraudulent charges on her bank account, requiring her to lock the account and request a new debit card. She temporarily lost her car insurance because her premium payment bounced while her account was locked, causing her to incur \$65 in fees. She also received notice from her credit monitoring service that her email address and SSN were compromised. ¶ 130.

3. Courtney Brown of Florida has noted unrecognized items on her credit report since the breach. Further, she was scheduled for surgery on the day of the breach, but the procedure could not be performed. ¶¶ 156, 162.

4. Mattie Boyden of Illinois received notice that her PII/PHI were on the dark web, and she has experienced an increase in spam calls, texts, and emails since the breach. ¶ 171.

5. Michael Cunningham of Kentucky received notice that his PII/PHI were on the dark web. He has seen fraudulent activity on his accounts and an increase in spam calls, texts, and emails since the breach. Further, he was forced to reschedule a medical procedure at a different hospital. ¶¶ 185, 187.

6. Leah Willis of Michigan was scheduled for a surgery that was postponed due to the breach, leaving her in pain in the interim. ¶ 200.

7. Cheryl Hayes of Oklahoma received notice that her PII/PHI were on the dark web, and she has seen an increase in spam calls, texts, and emails since the breach. She also experienced delay and difficulty refilling prescriptions. ¶¶ 214, 220.

8. Christina McClellan has seen an increase in spam calls, texts, and emails since the breach, personalized to her. ¶ 229.

9. Donald Pitchers of Indiana was unable to timely obtain insulin for his diabetes, forcing him to ration his supply. He was also informed that his PII/PHI were on the dark web. ¶¶ 243-244.

10. George Gounaris of Indiana was notified that his PII or PHI was found on the dark web. ¶ 257.

11. Jill Radley of Wisconsin incurred large withdrawals from her bank account and related overdraft fees. She has also seen an increase in spam calls, texts, and emails since the breach, personalized to her and related to her health issues. ¶ 271.

The breach occurred May 8, 2024. In December 2024, Ascension began notifying consumers that the compromised files included patients' names, birth dates, addresses, medical records, payment information (e.g. credit card and bank account numbers), insurance information, and government identification (e.g. social security, driver's license, and passport numbers). (Doc. 64 at 13 n.1).<sup>4</sup> The notice offered mitigation in the form of 24 months of credit monitoring, a \$1 million insurance policy, and identity theft recovery services.

Ascension now moves to dismiss the complaint for lack of subject matter jurisdiction under Rule 12(b)(1), Fed. R. Civ. P., arguing that Plaintiffs suffered no actual injury caused by the attack and therefore lack standing to sue. Alternatively, Ascension seeks to dismiss the complaint under Rule 12(b)(6) on various theories of unviability specific to each claim. Plaintiffs contend that their alleged injuries attributable to the breach – e.g., financial fraud, lost time, nuisance, intrusion, and ongoing vulnerability – establish standing and that their pleadings are sufficient to state a claim for relief under each theory asserted.

## **JURISDICTION**

### **Rule 12(b)(1)**

Rule 12(b)(1) permits a party to move for dismissal for lack of subject matter jurisdiction. The existence of subject matter jurisdiction is a question of law. *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 908 (8th Cir. 2016). When a motion to dismiss for lack of subject matter jurisdiction is brought at the pleading stage, the Court reviews it as a facial attack on jurisdiction. In this posture, the Court restricts itself to the face of the pleadings, accepting the allegations as true and drawing all inferences in the plaintiffs' favor. *In re SuperValu, Inc.*, 870 F.3d 763, 768 (8th Cir.

---

<sup>4</sup> [Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e55264f2-ff87-4b28-874d-653cfb735fe6.html), <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e55264f2-ff87-4b28-874d-653cfb735fe6.html> (last visited September 23, 2025).

2017).

If a plaintiff has no standing, then the district court has no subject matter jurisdiction, and the case must be dismissed pursuant to Rule 12(b)(1). *ABF Freight Sys., Inc. v. Int'l Broth. of Teamsters*, 645 F.3d 954, 958 (8th Cir. 2011). “Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). A plaintiff must demonstrate “that she has suffered an injury fact that is fairly traceable to the defendant’s conduct and that is likely to be redressed by the relief she seeks.” *In re SuperValu, Inc.*, 870 F.3d at 768 (citing *Spokeo*). “To establish an injury in fact, a plaintiff must show that her injury is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* When claiming future injuries, a plaintiff must demonstrate that the threatened injury is “certainly impending” or that there is a “substantial risk” that the harm will occur. *Id.* at 769.

These requirements apply to putative class actions. *Id.* at 768. Plaintiffs must demonstrate standing for each claim and for each form of relief they seek. *Murthy v. Missouri*, 603 U.S. 43, 61 (2024).

### **Nationwide Class Standing**

Ascension contends that Plaintiffs have not sufficiently pleaded actual injury or causation to establish standing. More specifically, it asserts that (1) Plaintiffs fail to connect bank and credit irregularities, spam, or dark web notices to the breach such that these harms are “fairly traceable” to it, (2) there are no claims of actual identity theft, and the risk of future theft is speculative and also minimal given Ascension’s corrective measures, and (3) the personal impacts of the breach identified in the complaint – the invasion of privacy, lost value of personal information, lost benefit of bargain, time spent mitigating and monitoring accounts and credit



reports, and the resulting stress and anxiety – aren’t cognizable injuries to create standing.

In response, Plaintiffs contend that all of the foregoing are adequately pleaded and cognizable injuries fairly traceable to Ascension for purposes of standing. In reply, Ascension concedes that suspicious bank and credit activity constitutes identity theft but maintains that Plaintiffs fail to connect those incidents to the breach.

Plaintiffs claim both present and future injuries. Some present injuries depend on the risk of future injury. For instance, time and money spent on monitoring and mitigation are cognizable only when the risk of future injury is substantial. *In re SuperValue*, 870 F.3d at 771. “In other words, this allegation is not in itself an injury in fact unless there is also a substantial risk of future injury in fact.” *Pulliam v. W. Tech. Grp., LLC*, 2024 WL 356777, at \*8 (D. Neb. Jan. 19, 2024). Likewise, emotional stress from a fear of a future harm is cognizable only when tethered to a substantial risk. *Id.* at \*10. Plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Murthy*, 603 U.S. at 73. As such, the Court first examines the risk of future harm.

#### Future Injury

In *SuperValu*, hackers gained access to the plaintiffs’ bank card information only. The Eighth Circuit held that the risk of future harm wasn’t substantial or imminent in that case because bank card information alone isn’t enough to open unauthorized new accounts. 870 F.3d at 770-71. The court specifically distinguished the scenario where stolen information includes PII such as SSNs, birth dates, and driver’s license numbers, reasoning that the type of data compromised can determine the potential harm. *Id.* at 770. In cases where precisely such highly exploitable PII *was* compromised, and some plaintiffs experienced actual instances of identity theft, other circuits have readily found a substantial risk of future injury for all plaintiffs. *Webb v.*

*Injured Workers Pharmacy, LLC*, 72 F.4th 365, 376 (1st Cir. 2023); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021). Consistent with that rationale, this Court and others in the Eighth Circuit recognize a substantial risk of future injury when a data breach involves SSNs and birth dates. *See, e.g., Mackey v. Belden, Inc.*, 2021 WL 3363174, at \*5 (E.D. Mo. Aug. 3, 2021); *Berry v. Crescent Cmty. Health Ctr.*, 2025 WL 1287909, at \*5 (N.D. Iowa May 2, 2025); *Perry v. Bay & Bay Transportation Servs., Inc.*, 650 F. Supp. 3d 743, 751 (D. Minn. 2023); *Coffey v. OK Foods Inc.*, 2022 WL 738072, at \*3 (W.D. Ark. Mar. 10, 2022); *Weisenberger v. Ameritas Mut. Holding Co.*, 597 F. Supp. 3d 1351, 1359 (D. Neb. 2022); *In re Pawn Am. Consumer Data Breach Litig.*, 2022 WL 3159874, at \*3-4 (D. Minn. Aug. 8, 2022). Some courts have found the risk of future injury too speculative in the absence of pleadings alleging actual fraudulent activity. *Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at \*4 (E.D. Mo. July 12, 2016); *Pulliam*, 2024 WL 356777, at \*7; *C.C. v. Med-Data Inc.*, 2022 WL 970862, at \*7 (D. Kan. Mar. 31, 2022).

Here, considering the nature of PII compromised, combined with multiple concrete incidents of suspicious bank and credit activity and dark web exposure after the breach, the Court finds the risk of future injury sufficiently substantial to establish standing. Further, given this real risk of future harm, Plaintiffs' dependent claims regarding time and money spent on mitigation and monitoring also confer standing. *SuperValu*, 870 F.3d at 774; *Webb*, 72 F.4th at 376-77; *In re Equifax*, 999 F.3d at 1263; *Mackey*, 2021 WL 3363174, at \*5; *Berry*, 2025 WL 1287909, at \*5. For the same reason, Plaintiffs have standing to pursue injunctive relief requiring Ascension to secure their information and provide mitigation services going forward. *Mackey*, 2021 WL 3363174, at \*12.

### Present Injury

Plaintiffs' present injuries vary in nature. Specific instances of fraudulent bank and credit activity are actual and concrete injuries. *See, e.g., SuperValu*, 870 F.3d at 772 (fraudulent credit card charge); *Mackey*, 2021 WL 3363174, at \*4 (fraudulent tax return); *Pawn*, 2022 WL 3159874, at \*4 (bank activity). Though Ascension contends that isolated incidents of suspicious bank or dark web activity could be attributed to other causes, Plaintiffs plead that these events occurred after and as a result of the breach and believe that their injuries are traceable to it. The Court accepts the pleadings as true at this early stage and finds them sufficient to entitle Plaintiffs to discovery on the issue. The Court also accepts at this stage that disruptions in medical care are cognizable for purposes of standing. Ascension's argument to the contrary is unpersuasive.<sup>5</sup>

However, Plaintiffs' alleged injuries in the form of spam calls, texts, and emails are not fairly traceable to Ascension. Phone numbers and email addresses weren't identified in the pleadings or public notices as types of PII compromised in the breach. Even if they were – and one would assume Ascension had them – such basic contact information can be obtained from any number of sources. To the extent Plaintiffs claim lost time or nuisance as a result of spam, the Court finds the connection to this data breach too speculative to establish standing entitling Plaintiffs to any form of relief. *See Berry*, 2025 WL 1287909, at \*5 (where the pleadings didn't link spam to the breach).

---

<sup>5</sup> Ascension cites two out-of-circuit cases that are inapposite. *Thomas v. Baker* involved a *pro se* plaintiff claiming injury from a delay in medical treatment attributable to the governor's executive orders issued in response to the acute stage of the COVID-19 pandemic. *Thomas v. Baker*, 2020 WL 6870994, at \*1 (D. Mass. Nov. 23, 2020). In *Crumb v. Orthopedic Surgery*, the court's finding that the plaintiff suffered no injury from delayed treatment was made at the summary judgment stage on a full record. *Crumb v. Orthopedic Surgery Med. Grp.*, 2010 WL 11509292, at \*6 (C.D. Cal. Aug. 18, 2010).

Benefit of Bargain

Next, in connection with their contract and MMPA claims, Plaintiffs allege harm from the lost benefit of their bargain with Ascension. With respect to this theory, the Court must be careful not to conflate the injury requirement for standing with the substance of Plaintiffs' cause of action. "A party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged." *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 716 (8th Cir. 2017) (citation omitted). Mindful of this distinction, the Court accepts Plaintiffs' pleading that a contract existed and thus they have standing to claim this injury. *See also Berry*, 2025 WL 1287909, at \*7; *Harris v. Mercy Health Network, Inc.*, 2024 WL 5055556, at \*8 (S.D. Iowa June 26, 2024) (recognizing plaintiffs' standing to assert contract claims based on a hospital's privacy policy but dismissing them on the merits); *K.A. by & Through B.W. v. Children's Mercy Hosp.*, 2019 WL 2144815, at \*3-5 (W.D. Mo. May 16, 2019) (accepting breach of contract and MMPA pleadings for purposes of standing but dismissing contract claim on the merits).

Invasion of Privacy

Opinions diverge as to whether a data breach confers standing to claim an invasion of privacy. The district courts in *Berry* and *Pawn* concluded without analysis that it does. *See also Medoff v. Minka Lighting, LLC*, 2023 WL 4291973, at \*3 (C.D. Cal. May 8, 2023) (analogizing the claim to the common law tort of public disclosure of private facts). Conversely, a court in this district found that a loss of privacy isn't a concrete and particularized harm for purposes of standing. *Duqum*, 2016 WL 3683001, at \*8. *Accord, C.C. v. Med-Data*, 2022 WL 970862, at \*10 (acknowledging that every data breach involves a loss of privacy but finding that the loss isn't concrete, citing *Duqum*). Other courts have reached the same result for different reasons

touching on the merits. *Pulliam*, 2024 WL 356777, at \*9 (referring to common law elements and finding that the information wasn't technically published, didn't concern the plaintiffs' private life, and wasn't highly offensive); *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at \*8 (W.D.N.Y. Feb. 2, 2022) (reasoning that the facts didn't fit the common law elements and the loss of privacy was too abstract).

This Court finds logic across the spectrum but again must distinguish standing from substance. There is no dispute that Plaintiffs lost the security of highly sensitive personal information as a result of this data breach. To the extent Plaintiffs plead emotional harm from this violation, this is a long-recognized injury flowing from an invasion of privacy. *Pawn*, 2022 WL 3159874, at \* 4 (collecting cases). As such, the Court finds that Plaintiffs at least have standing to assert this claim. The Court reserves for the merits whether the present facts fit the common law elements to state a claim.

#### Lost Value of PII

Here, too, opinions vary as to whether plaintiffs suffer a cognizable loss of value of their PII as a result of a data breach. Some districts in this circuit have assumed without much examination that it does. *See, e.g., Perry*, 650 F. Supp. 3d at 757; *Hall v. Centerspace, LP*, No. 22-CV-2028 (KMM/DJF), 2023 WL 3435100, at \*8 (D. Minn. May 12, 2023); *Rodriguez v. Mena Hosp. Comm'n*, 2023 WL 7198441, at \*6 (W.D. Ark. Nov. 1, 2023). Conversely, in *Duqum*, the court found no injury because the information had no market value. *Duqum*, 2016 WL 3683001, at \*7. *Accord, Taylor v. UKG, Inc.*, 693 F. Supp. 3d 87, 101 (D. Mass. 2023) (reasoning that plaintiffs had not attempted to sell their data and received a lower price). In *Pulliam*, the court acknowledged the practical value of personal information but found no traditional analogue at common law and thus deemed the loss insufficiently concrete to confer

standing. *Pulliam*, 2024 WL 356777, at \*8. In this Court’s view, the practical value is significant.

Plaintiffs offer a useful analysis in *In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020). There, the data breach involved the theft of hotel guests’ personal and payment information. Finding a cognizable injury in fact, the court explained that the value of the information isn’t derived from its worth in an “imagined marketplace” but rather in the economic benefit of being able to purchase goods and services remotely and electronically.

[The Court should not] ignore what common sense compels it to acknowledge – the value that personal identifying information has in our increasingly digital economy. Many companies ... collect personal information. Consumers, too, recognize the value of their personal information and offer it in exchange for goods and services. ... Further, the value of personal identifying information is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their personal identifying information. Here Plaintiffs allege that they suffered lower credit scores as a result of the data breach and that fraudulent accounts and tax returns were filed in their names. Similarly, the businesses that request (or require) consumers to share their personal identifying information as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

*Id.* at 462 (cleaned up). The Court finds this rationale logical and persuasive. The fact that certain intangible damages don’t lend themselves to precise market valuation doesn’t render the injury any less real to the victim of a data breach. *See also Gordon v. Zeroed-In Tech., LLC*, 2025 WL 936415, at \*7 (D. Md. Mar. 26, 2025) (reasoning that the breach impeded plaintiffs’ ability to participate in the economy). The Court finds that the lost value of Plaintiffs’ information is a concrete injury in fact for purposes of standing.

## **SUFFICIENCY OF THE COMPLAINT**

### **Rule 12(b)(6)**

To survive a motion to dismiss under Rule 12(b)(6), “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) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570 (2007)). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. When considering a Rule 12(b)(6) motion to dismiss, the court must accept the allegations contained in the complaint as true, and all reasonable inferences from the complaint must be drawn in favor of the nonmoving party. *Ringhofer v. Mayo Clinic, Ambulance*, 102 F.4th 894, 901 (8th Cir. 2024). Courts are not bound to accept as true a legal conclusion couched as a factual allegation, and factual allegations must be enough to raise a right to relief above the speculative level. *Torti v. Hoag*, 868 F.3d 666, 671 (8th Cir. 2017). Legal conclusions or formulaic recitations of the elements of a cause of action do not suffice. *DeCastro v. Hot Springs Neurology Clinic, P.A.*, 107 F.4th 813, 816 (8th Cir. 2024).

Review of the complaint on a motion to dismiss is a context-specific task that requires the court to draw on its judicial experience and common sense. *Norfolk & Dedham Mut. Fire Ins. Co. v. Rogers Mfg. Corp.*, 122 F.4th 312, 315 (8th Cir. 2024) (citing *Iqbal*, 556 U.S. at 679). A “well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and that a recovery is very remote and unlikely.” *Id.*

Negligence (Count I)

Plaintiffs plead that, by virtue of a special patient-provider relationship, Ascension had a duty to employ reasonable measures, consistent with industry standards, to secure and protect Plaintiffs' PII/PHI from this foreseeable data breach. More specifically, Plaintiffs cite industry standards contained in the HIPAA regulations and FTC guidelines, as described in the introduction.

In support of its motion to dismiss this count, Ascension argues that Plaintiffs' negligence claim is precluded by the economic loss doctrine, which bars the recovery of purely pecuniary losses in tort where the injury results from a breach of contract. *Mackey*, 2021 WL 3363174, at \*7. Ascension simultaneously disputes the existence of any contract. As discussed further below, the Court agrees that the pleadings fail to establish an express or implied contract. Even acknowledging conflicting caselaw recognizing implied contracts in the data breach context, Plaintiffs' negligence claim would still survive here because the economic loss doctrine doesn't apply when there's a special relationship between the parties. *Id.* at \*8; *Emerson Elec. Co. v. Marsh & McLennan Companies*, 362 S.W.3d 7, 12 n.4 (Mo. 2012).

In *Mackey*, this Court accepted that an employment relationship was sufficiently special to give rise to an employer's duty to protect employees' PII from a data breach. *Mackey*, 2021 WL 3363174, at \*8. Given the highly sensitive nature of PHI shared in the health care context, the patient-provider relationship is even more sacred and is clearly recognized as special under Missouri law. *J.J. by & through C.W. v. Poplar Bluff Reg'l Med. Ctr., L.L.C.*, 675 S.W.3d 259, 266 (Mo. App. E.D. 2023) (stating that a doctor's fiduciary duty of confidentiality to patients extends to all employees in a health care setting). *Accord, Pollack v. Cruz*, 296 So. 3d 453, 460 (Fla. Dist. Ct. App. 2020) (recognizing a special relationship between hospitals and patients).



Disputing this characterization, Ascension argues that the patient-provider fiduciary relationship and resulting duty of confidentiality applies only to individual doctors, not to institutions. In support, Ascension cites *Cahill v. Mem'l Heart Inst., LLC*, 2024 WL 4311648, at \*14 (E.D. Tenn. Sept. 26, 2024), where the court reasoned that the plaintiffs merely purchased medical services from the defendant hospital in a commercial transaction. This Court does not share that logic. In the context of a systemwide data breach, it makes no sense to recognize the fiduciary duty of a patient's doctor but not of the entity maintaining the treatment records. In the Court's view, the level of trust inherent in the patient-provider relationship and corresponding duty of confidentiality codified by HIPAA necessarily extends to regulated providers and warrants fiduciary treatment.<sup>6</sup>

As such, the Court concludes that the economic loss doctrine wouldn't bar Plaintiffs' negligence claim even if their contract claims were viable. Ascension's motion to dismiss will be denied as to Count I.

#### Negligence Per Se (Count II)

"Negligence *per se* 'is a form of ordinary negligence that results from violation of a statute' and 'arises where the legislature pronounces in a statute what the conduct of a reasonable person must be.'" *Aubuchon v. Tate Trucking, LLC*, 2024 WL 4285880, at \*2 (E.D. Mo. Sept. 25, 2024) (quoting *Lowdermilk v. Vescovo Bldg. & Realty Co., Inc.*, 91 S.W.3d 617, 628 (Mo. App. E.D. 2002)). It is "in effect a presumption that one who has violated a safety statute has violated his legal duty to use due care." *J.J.'s Bar & Grill, Inc. v. Time Warner Cable Midwest*,

---

<sup>6</sup> The other cases cited in Ascension's brief didn't involve HIPAA and thus don't change the Court's conclusion. See *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 818 (7th Cir. 2018) (where plaintiff was a bank and defendant was a grocery chain); *Sherman v. Sea Ray Boats, Inc.*, 649 N.W.2d 783 (2002) (involving the sale of a boat); *U.S. Bank, N.A. v. Integrity Land Title Corp.*, 929 N.E.2d 742, 744 (Ind. 2010) (where a bank sued a title company).

*LLC*, 539 S.W.3d 849, 868 (Mo. App. W.D. 2017). “To establish a claim of negligence *per se*, the plaintiff must plead and prove the following four elements: (1) the defendant violated a statute; (2) the injured plaintiff was a member of the class of persons intended to be protected by the statute; (3) the injury complained of was of the kind the statute was designed to prevent; and (4) the violation of the statute was the proximate cause of the injury.” *Martinez v. Kilroy Was Here LLC*, 551 S.W.3d 491, 496 (Mo. App. E.D. 2018). “When a case based on negligence *per se* is submitted to the jury, the standard of care is omitted because the statutory violation itself constitutes a breach of the standard of care.” *Dibrill v. Normandy Assocs., Inc.*, 383 S.W.3d 77, 84 (Mo. App. E.D. 2012).

Plaintiffs assert a claim of negligence *per se* based on Ascension’s violation of HIPAA and the FTCA. Specifically, HIPAA requires a covered entity to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of [PHI].” 45 C.F.R. § 164.530(c)(1). As further summarized in the introduction, the regulations impose numerous standards and implementation specifications relating to particular security considerations and requiring appropriate institutional procedures and practices. *See, e.g.*, 45 C.F.R. § 164.306, § 164.308, § 164.312. The FTCA prohibits unfair and deceptive trade practices, 15 U.S.C. § 45, and the FTC’s resource *Protecting Personal Information: A Guide for Business* recommends precautions and practices for the retention, protection, and disposal of information. (Doc. 52 at 20-21).

In support of its motion to dismiss this count, Ascension contends that negligence *per se* lies only where a statute creates a private cause of action, and neither HIPAA nor the FTCA creates one. As the Court understands it, Ascension posits that a plaintiff must have a statutory claim in order to also have a negligence claim. This is incorrect. “The test to determine whether a

violation of a statute may constitute negligence per se depends on legislative intent.” *J.J.'s Bar & Grill, Inc. v. Time Warner Cable Midwest, LLC*, 539 S.W.3d 849, 869 (Mo. App. W.D. 2017).

“There is a difference between whether a statute creates a private cause of action permitting an individual to initiate a lawsuit ... based on a violation of the statute, and whether a statute establishes a standard of care supporting recovery on a theory of negligence per se because a violation of the statute relieves the jury of the obligation to find negligence.” *Id.* at 866 n.13.

Indeed, it would make no sense for a common law claim of negligence *per se* to lie only where a statutory claim already exists. A statutory “cause of action” isn’t a *prima facie* element for negligence *per se*. Rather, the inquiry is simply whether the legislature (or regulatory body) intended for the statute to establish the standard of care. *Id.* The “initial question is whether the legislation or regulation is to be given any effect in a civil suit.” *Id.* at 869 (quoting the Restatement (Second) of Torts § 286 comment d.).

On this question, the Missouri Court of Appeals has recognized that HIPAA creates a statutory duty of confidentiality that, when violated, gives rise to a common law claim of negligence *per se* under Missouri law. *J.J.*, 675 S.W.3d at 266. Upon review of the HIPAA regulations cited by Plaintiffs, which impose numerous mandatory standards and implementation specifications across a range of information security considerations, this Court agrees that the statute and corresponding regulations were intended to establish a legal duty and standard of care for the protection of patients’ personal information.

By contrast, the Eighth Circuit has concluded that the FTCA does not create a legal duty enforceable through a state negligence action. *In re SuperValu, Inc.*, 925 F.3d 955, 964 (8th Cir. 2019) (applying Illinois common law). Indeed, neither the statutory language of the FTCA nor the FTC publication, *Protecting Personal Information: A Guide for Business*, which Plaintiffs

cite as the source of industry “guidelines,” can be interpreted to legislate a standard of care for data security. The FTCA simply prohibits unfair and deceptive trade practices, and the guide merely recommends security best practices for the inventory, retention, protection, and disposal of information as well as crisis management planning.

Accordingly, the Court finds that Plaintiffs have stated a viable claim for negligence *per se* based on alleged violations of HIPAA and applicable regulations but not based on the FTCA or the FTC *Guide for Business*. Ascension’s motion to dismiss will be granted in part and denied in part on this Count II.<sup>7</sup>

#### Breach of Express Contract (Count III)

In Count III, Plaintiffs plead that they had an express contract with Ascension in the form of its Notice of Privacy Practices, which advises patients of their rights and Ascension’s obligations under HIPAA and explains the parameters of Ascension’s use of patient PII/PHI. They assert that the contract was formed when they obtained services and provided their PII/PHI subject to the Notice. Plaintiffs plead that the Notice constitutes a written agreement, which Ascension breached by failing to protect Plaintiffs’ PHI/PII. In support of its motion to dismiss this count, Ascension argues that the complaint lacks facts demonstrating the elements of mutual assent and consideration required to form a contract.

To determine whether an agreement is formed, courts look for the essential elements of a contract: offer, acceptance, consideration, and whether there was a meeting of the minds and mutual assent to the essential terms of the agreement. *Woodson v. Bank of Am., N.A.*, 602 S.W.3d 316, 323 (Mo. App. E.D. 2020). “Mutuality of agreement is determined by looking at both the

---

<sup>7</sup> The parties don’t ask the Court to conduct a choice-of-law analysis at this time but seem to agree that the states of Arkansas, Kentucky, and Michigan do not recognize a cause of action for negligence *per se* based on federal statutory standards of care, though such standards are relevant to a finding of ordinary negligence.

intentions of the parties as expressed or manifested in their words or actions and the circumstances surrounding the parties' relationship." *Id.* (cleaned up).

In *Kuhns*, the Eighth Circuit rejected the notion that a portion of payment for brokerage services was for data security pursuant to a privacy policy. 868 F.3d at 718. In the HIPAA context, the Western District of Missouri dismissed the theory that a privacy policy constitutes a contract because the statutory obligation to comply with HIPAA requires no consideration. *K.A. by & through B.W. v. Children's Mercy Hosp.*, No. 18-00675-CV-W-ODS, 2019 WL 13207485, at \*6 (W.D. Mo. May 17, 2019). *Accord, Harris*, 2024 WL 5055556, at \*10; *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1221 (S.D. Fla. 2022); *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1367 (S.D. Fla. 2017).<sup>8</sup>

The Court agrees with this reasoning. Plaintiffs' bare allegation that the Notice constitutes an agreement is conclusory. The Notice is merely a notice, informing patients of their rights under HIPAA and the duties HIPAA imposes on providers. *Mednax*, 603 F. Supp. 3d at 1221-22. Plaintiffs do not and could not plead that they understood the Notice to create a contract for data security funded by their payment for medical services. Any provider's itemization of charges dispels that belief. *See SuperValu II*, 925 F.3d at 966 (rejecting the concept of PII as a benefit conferred in exchange for data protection). But even accepting this illogical premise, assent must still be mutual to form a contract, and the complaint doesn't and couldn't allege a contractual undertaking or assent by Ascension when its privacy obligations are statutory and cannot be purchased or bargained for. *K.A.*, 2019 WL 13207485, at \*6; *Mednax*,

---

<sup>8</sup> Conversely, in *Weisenberger v. Ameritas Mut. Holding Co.*, 597 F. Supp. 3d 1351, 1359 (D. Neb. 2022), the court found sufficient consideration by characterizing the agreement as "If you give us your PII, we will keep it secure pursuant to our duty under HIPAA." This Court does not share that view.

603 F. Supp. 3d at 1222. Count III fails to state a claim and will be dismissed.

Breach of Implied Contract (Count IV)

Absent an express contract, Plaintiffs plead that the parties had an implied contract pursuant to which Ascension agreed to safeguard their PII/PHI in accordance with industry standards. They assert that Ascension violated an implied covenant of good faith and fair dealing by failing to maintain adequate data security.

“There is no difference in legal effect between an express contract and one implied in fact. The distinction lies merely in the manner of manifesting mutual assent.” *Nickel v. Stephens College*, 480 S.W.3d 390, 397 n.6 (Mo. App. W.D. 2015) (internal citation omitted). To determine whether an implied contract exists, courts consider the parties’ acts, conduct, and statements as a whole; whether there was a meeting of the minds on essential elements; the parties’ intent to enter into a contract upon defined terms; and whether one of the parties has relied in good faith on the alleged contract. *Id.*

Plaintiffs plead that the parties’ mutual understanding on the essential terms of their agreement is evidenced by their course of conduct and Ascension’s statements in the Notice. Specifically, Plaintiffs provided their PII/PHI in order to receive services; Ascension accepted the information and promised to protect it; Plaintiffs paid Ascension for health care services; and Plaintiffs expected Ascension to use part of its earnings for data security.

In support of its motion to dismiss this count, Ascension argues that the complaint cannot establish mutual assent and consideration. The Court agrees for the same reasons stated above with respect to express contracts. Ascension’s obligation to protect Plaintiffs’ information is entirely statutory, not transactional. The cases cited by Plaintiffs don’t involve HIPAA and are factually distinguishable in that important regard. *Mackey*, 2021 WL 3363174 at \*8 (involving

PII retained by the plaintiff's employer); *Hall v. Centerspace, LP*, No. 22-CV-2028 (KMM/DJF), 2023 WL 3435100, at \*5 (D. Minn. May 12, 2023) (same); *Baldwin v. Nat'l W. Life Ins. Co.*, 2021 WL 4206736, at \*7 (W.D. Mo. Sept. 15, 2021) (PII provided to purchase life insurance); *Mohsen v. Veridian Credit Union*, 733 F. Supp. 3d 754, 768 (N.D. Iowa 2024) (PII deemed exchanged for banking services beneficial to the bank); *Hiscox Ins. Co. Inc. v. Warden Grier, LLP*, 474 F. Supp. 3d 1004, 1010 (W.D. Mo. 2020) (PII provided to law firm).<sup>9</sup>

Again, the complaint cannot be understood to demonstrate Ascension's contractual assent or acceptance of any form of consideration for data security. *K.A.*, 2019 WL 13207485, at \*6; *Mednax*, 603 F. Supp. 3d at 1222. Absent an implied contract, there is also no implied covenant of good faith and fair dealing. Count IV fails to state a claim and will be dismissed.

#### Unjust Enrichment (Count V)

In the alternative to their implied contract claim, Plaintiffs assert a claim for unjust enrichment, which "requires a showing that (1) the plaintiff conferred a benefit on the defendant; (2) the defendant appreciated the benefit; and (3) the defendant accepted and retained the benefit under inequitable and/or unjust circumstances." *Hargis v. JLB Corp.*, 357 S.W.3d 574, 586 (Mo. 2011) (cleaned up). Plaintiffs plead that they conferred benefits on Ascension in the form of payment for services and PII/PHI in connection therewith, and Ascension retained those benefits inequitably by failing to secure Plaintiffs' information. Plaintiffs submit that, by neglecting to invest in adequate security, Ascension unjustly profited at their expense.

In support of its motion to dismiss on this count, Ascension argues that Plaintiffs paid for health care services, not data security, and PII/PHI is not a benefit to the provider. Plaintiffs

---

<sup>9</sup> In *Hiscox*, the law firm arguably had an ethical duty to protect confidential information in a manner not subject to contractual consideration. 474 F. Supp. 3d at 1010. The Court nonetheless finds this case less persuasive than those specifically involving violations of HIPAA.

counter that providing their PII/PHI was a condition of receiving care and thus not severable from the benefit of payment.

Though there is some variation in existing caselaw, the majority appears to reject Plaintiffs' theory. Most notably, in *SuperValu II*, the Eighth Circuit reasoned that the defendant didn't receive a benefit in exchange for data security because no portion of payment was attributable to that service. *SuperValu II*, 925 F.3d 966. Several district courts in this circuit have applied this reasoning in a HIPAA context. *See, e.g., Berry*, 2025 WL 1287909, at \*10; *Harris*, 2024 WL 5055556, at \*12; *Rodriguez v. Mena Hosp. Comm'n*, 2023 WL 7198441, at \*11 (W.D. Ark. Nov. 1, 2023) (also rejecting the "would not have shopped" theory).

The cases cited by Plaintiffs are distinguishable and unpersuasive. In *In re Group Health Plan Litig.*, 709 F. Supp. 3d 707, 715 (D. Minn. 2023), the defendant health care company exploited patients' PII/PHI by tracking their website activity and providing that data to Facebook, thus clearly deriving a commercial benefit. In *Mohsen*, the court accepted without analysis that a bank benefited from its customers' PII.<sup>10</sup> 733 F. Supp. 3d at 768. Consistent with *SuperValu II*, *Berry*, *Harris*, and *Rodriguez*, the Court will grant Ascension's motion to dismiss as to Count V.

---

<sup>10</sup> This Court questions whether patients' PII/PHI confers a separate benefit on providers in a contractual sense. As a practical matter, most PHI is generated by the provider. And to the extent patients supply PII/PHI, it benefits *patients* by facilitating care and creates additional *burdens* for the provider, whose only benefit in the transaction is the payment for health care services. This is materially different from a scenario where, for example, a consumer provides PII to a commercial vendor in exchange for a discount or goods and services, enabling the vendor to then use that PII for marketing purposes. *See In re Mednax*, 603 F. Supp. 3d at 1221 (contrasting consumer transactions and health care services).



Invasion of Privacy (Count VI)

Missouri law recognizes four variations on a claim for invasion of privacy. Plaintiffs invoke two.<sup>11</sup> Tortious “intrusion on seclusion” has three elements: (1) an intentional intrusion (2) on the private affairs of another (3) by unreasonable means and highly offensive to a reasonable person. *Sofka v. Thal*, 662 S.W.2d 502, 510 (Mo. banc 1983) (citing the Restatement (Second) of Torts § 652B). Publication isn’t an element on this theory. *Id.* It merely requires a subject matter that the plaintiff is entitled to keep private and the defendant’s acquisition of such information through unreasonable means. *Ryno v. Hillman*, 641 S.W.3d 385, 393 (Mo. App. S.D. 2022). Alternatively, “public disclosure of private facts” involves (1) the defendant’s publication to a large number of persons (2) absent a grant to the defendant of any waiver or privilege (3) the disclosure of private matters in which the public has no legitimate concern (4) in a way as to bring shame or humiliation to an individual of ordinary sensibilities. *Y.G.*, 795 S.W.2d at 498-99 (where a hospital disclosed a patient’s IVF treatment to the media); *J.J.*, 675 S.W.3d at 262 n.3 (where a hospital employee disclosed a minor’s medical information to his schoolmate).

While Plaintiffs have surely suffered an appropriation of their private information, these legal theories don’t fit the present facts. First, Ascension didn’t commit the intrusion or publication; hackers did. By imputing the conduct to Ascension due to its inadequate security, Plaintiffs essentially reprise their negligence claim. But this attempt to convert omission into action doesn’t comport with the facts or relevant elements. The intrusion was perpetrated by a cybercriminal, not Ascension. Second, the Court is not persuaded that a criminal cyberattack equates to “publication” in the common law sense. Put simply, the actual actor and proper

---

<sup>11</sup> The two theories not applicable here are (1) appropriation of a plaintiff’s name or likeness and (2) publicity placing the plaintiff in a false light. *Y.G. v. Jewish Hosp. of St. Louis*, 795 S.W.2d 488, 498 (Mo. App. E.D. 1990) (citing the Restatement (Second) of Torts § 652C and E).

defendant for this count is not a party. Plaintiffs' claim is properly framed as negligence.

Ascension's motion to dismiss will be granted as to Count VI.

### **State Statutory Claims**

Plaintiffs assert twelve separate counts under the consumer protection statutes of Missouri, Arkansas, Florida, Illinois, Oklahoma, Wisconsin, Michigan, and Indiana.

#### **Missouri Merchandising Practices Act (Count VII)**

As relevant here, the MMPA prohibits misrepresentations and the concealment or omission of material facts "in connection with" the sale of services and creates a civil action for any buyer who suffers an ascertainable loss "as a result of" the use of an unlawful practice. Mo. Rev. Stat. § 407.010(4), § 407.020, § 407.025. An "unfair practice" is defined to include unethical practices that present a risk of or cause substantial injury to consumers. 15 C.S.R. § 60-8.020.

Plaintiffs plead that Ascension violated the MMPA by misrepresenting that it would protect PII/PHI in compliance with HIPAA and concealing the fact that its data security was inadequate. Plaintiffs further plead that Ascension's failure to meet industry standards constitutes an unethical and unfair practice that presents a risk to consumers. In support of its motion to dismiss this count, Ascension contends that Plaintiffs' allegations fail to satisfy the heightened pleading standards of Rule 9(b), Fed. R. Civ. P., because Plaintiffs don't specifically identify any actionable misrepresentation or omission, and they don't claim to have relied on the Notice.

"The Eastern and Western Districts of Missouri have consistently held that Rule 9(b) applies to MMPA cases." *Brunts v. Hornell Brewing Co.*, 2023 WL 3568650, at \*9 (E.D. Mo. May 19, 2023). "When Rule 9(b) applies, the complaint must allege such matters as the time, place, and contents of the false representations, as well as the identity of the person making the

misrepresentation and what was obtained or given up thereby.” *Collins v. Metro. Life Ins. Co.*, 117 F.4th 1010, 1017 (8th Cir. 2024). In other words, the party must identify the “who, what, where, when, and how.” *BJC Health Sys. v. Columbia Cas. Co.*, 478 F.3d 908, 917 (8th Cir. 2007). Rule 9 is to be interpreted “in harmony with the principles of notice pleading.” *Schaller Tel. Co. v. Golden Sky Sys., Inc.*, 298 F.3d 736, 746 (8th Cir. 2002). A complaint subject to Rule 9 need not provide anything more than notice of the claim; it simply requires a higher degree of notice enabling the defendant to respond to potentially damaging allegations. *Id.* “The level of particularity required depends on the nature of a case.” *E-Shops Corp. v. U.S. Bank Nat’l Ass’n*, 678 F.3d 659, 663 (8th Cir. 2012).

Ascension’s HIPAA Notice itself, incorporated by reference into the complaint, states that Ascension is “committed to maintaining the privacy and confidentiality of your health information” and “required by law” to do so. (Doc. 73-1). Plaintiffs characterize this as a misrepresentation that Ascension would protect the privacy and confidentiality of Plaintiffs’ PII/PHI by maintaining adequate security. Ascension argues that Plaintiffs fail to explain how these statements are false, citing *Feins v. Goldwater Bank NA*, 2022 WL 17552440, at \*8 (D. Ariz. Dec. 9, 2022). There, the privacy policy represented that the defendant bank would protect personal information from unauthorized access and use security measures that comply with federal law. The court found those statements insufficient, reasoning that the data breach itself was not enough to show that the statements were false. However, in *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 776 (W.D.N.Y. 2017), the court found substantially similar representations by a HIPAA-regulated entity sufficient because they would lead a reasonable consumer to believe that the defendant was providing adequate data security. Similarly, the MMPA provides relief when the representation in question would cause a reasonable person to

enter into the transaction. § 407.025. Given the language of Ascension’s Notice within the broader context of patient-provider confidentiality and HIPAA, a consumer could reasonably understand and rely on the Notice to mean that Ascension protects PII/PHI. The Court accepts the sufficiency of Plaintiffs’ pleadings at this early stage.

From here, Plaintiffs centrally allege that, in the course of their treatment (the “when” and “where”), Ascension represented to them in the Notice that it would keep their PII/PHI private; they relied on Ascension to do so; Ascension concealed the fact that its security was inadequate; and they wouldn’t have provided their PII/PHI had they known of Ascension’s inadequate security. As a whole, the 120-page complaint lays out sufficient facts to enable Ascension to respond to the allegations. Ascension cannot claim ignorance of the dates and locations of each plaintiff’s treatment. Such granular details in Ascension’s possession are unnecessary to place it on notice of Plaintiffs’ class claims. Given the nature of this case, the Court finds the pleadings sufficiently specific to provide Ascension notice of the claim. *Schaller*, 298 F.3d at 746. To the extent Ascension reprises this theory on Plaintiffs’ other state statutory claims, the Court reaches the same conclusion.

However, Plaintiffs’ MMPA still fails for a different reason. The Eighth Circuit’s decision in *Kuhns* is directly on point and fatal to this count. There, according to the complaint, the defendant brokerage company represented in privacy statements that it would protect clients’ information, but the company failed to maintain adequate cybersecurity measures and suffered a cyberattack. 868 F.3d at 717. Noting that the MMPA requires an unlawful act and pecuniary loss “in relation to” a sale and purchase of a service, the Eighth Circuit concluded that the plaintiffs’ MMPA claim wasn’t viable because the plaintiff purchased brokerage services, not data security. *Id.* at 719. Thus, the alleged misrepresentation and corresponding loss didn’t “relate to” the

purchase of information privacy.

The Missouri Supreme Court appears to share the Eighth Circuit’s reasoning that services not contemplated as part of the transaction are not included “in connection with” it for purposes of MMPA liability. *See Jackson v. Barton*, 548 S.W.3d 263, 271 (Mo. 2018) (holding that debt collection services were included “in connection with” the sale because they involved recovering payment to complete the sale), and *Watson v. Wells Fargo Home Mortg., Inc.*, 438 S.W.3d 404, 408 (Mo. 2014) (holding that loan modification negotiations weren’t included “in connection with” the sale of the loan because they weren’t a service that the lender agreed to sell and the borrower agreed to buy). More recently, a Missouri appellate court suggested in *dicta* that a healthcare provider’s breach of confidentiality could indeed give rise to liability under the MMPA. *J.J.*, 675 S.W.3d at 266. However, absent clear precedent to that effect, this Court must follow *Kuhns* as further informed by *Jackson* and *Watson*. Consequently, Ascension’s motion will be granted as to Count VII.

Arkansas Deceptive Trade Practices Act (Count VIII)

Plaintiff Linda Dunn, on behalf of the Arkansas subclass, asserts a claim under the Arkansas Deceptive Trade Practices Act (ADTPA), Ark. Code. Ann. §§ 4-88-101, *et seq.* Much like the MMPA, ADTPA prohibits the use of deception or the concealment or omission of material fact with the intent that others rely on it. § 4-88-108. Plaintiffs allege that Ascension engaged in unconscionable practices, in violation of § 4-88-107(10), by misrepresenting that it would protect PII/PHI, concealing the inadequacy of its systems, and failing to maintain adequate security as required by the Arkansas Personal Information Protection Act, § 4-110-104.

In support of its motion to dismiss on this count, Ascension first argues that ADTPA prohibits class actions except when the claim involves a violation of the state constitution. § 4-

88-113(f)(1)(B). In response, Plaintiffs cite *Mounce v. CHSPSC, LLC*, where the district court allowed an ADTPA class action to proceed notwithstanding the statutory prohibition, reasoning that Rule 23 is procedural and supersedes any conflicting state procedural law. 2017 WL 4392048, at \*7 (W.D. Ark. Sept. 29, 2017) (citing *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 409-10 (2010)). See also *Whitley v. Baptist Health*, 2020 WL 4575991, at \*1 (E.D. Ark. Aug. 7, 2020) (noting that Rule 23 trumps ADTPA’s class action prohibition). Upon review of these cases, the Court agrees that § 4-88-113(f)(1)(B) cannot preclude Plaintiff Dunn’s putative class claim in federal court.

Ascension also invokes its global theory that Plaintiff Dunn fails to satisfy the heightened pleading standards of Rule 9(b). See e.g., *Jarrett v. Panasonic Corp. of N. Am.*, 8 F. Supp. 3d 1074, 1085 (E.D. Ark. 2013) (applying Rule 9(b) to an ADTPA claim). Ascension specifically argues that Plaintiffs have not sufficiently pleaded their reliance on an actionable misrepresentation or omission that caused injury. (Doc. 60 at 40-42). But the complaint expressly alleges these elements on this count. (See Doc. 52 at 91-93). As stated above with respect to Plaintiffs’ MMPA claim, given the particular nature of this case, the totality of the pleadings, and the further details in Ascension’s possession, the Court finds the pleadings sufficiently specific to place Ascension on fair notice of Plaintiffs’ claims in accordance with Rule 9(b).

Ascension’s motion to dismiss will be denied as to Count VIII.

Florida Deceptive and Unfair Trade Practices Act (Count IX)

Plaintiff Courtney Brown, on behalf of the Florida subclass, asserts a claim under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA), which simply states that unconscionable, unfair, or deceptive trade practices are unlawful. Fla. Stat. §§ 501.204. In construing the statute, “due consideration and great weight” is given to interpretations of the

FTCA, 15 U.S.C. § 45. Plaintiff Brown pleads that Ascension violated the FDUTPA by misrepresenting that it would protect her PII/PHI and concealing its inadequate security. She further pleads that Ascension violated its legal duty under a separate statute, § 501.171, to take reasonable measures to protect electronic data containing personal information. Plaintiff Brown had a surgical procedure canceled as a result of the breach, and her credit report was impacted.

In support of its motion to dismiss this count, Ascension again raises its global theory of insufficient pleadings with respect to reliance on an actionable representation or omission. Rule 9(b) doesn't apply to FDUTPA claims. *Harris v. Nordyne, LLC*, 2014 WL 12516076, at \*5 (S.D. Fla. Nov. 14, 2014). And in any case, the Court finds the pleadings sufficient.

Ascension also argues that FDUTPA applies only to conduct that occurs in Florida, which can't be the case here because Plaintiffs plead for purposes of venue that Ascension is based in Missouri and maintained patients' PII/PHI in Missouri. Indeed, Florida federal courts confirm that FDUTPA claims "must arise out of conduct that occurred within the state of Florida." *Lingard v. Holiday Inn Club Vacations, Inc.*, 2023 WL 4661963, at \*11 (M.D. Fla. July 20, 2023). But Plaintiffs' venue pleadings don't negate the facts giving rise to their FDUTPA claim. Venue is a separate inquiry and is proper in the district where the defendant resides *or* where a substantial part of events occurred. 28 U.S.C. § 1391(b). The complaint is readily understood to allege that the Florida resident Plaintiffs were treated at Ascension facilities in Florida. Necessarily, then, these Plaintiffs received Ascension's HIPAA Notice and provided their PII/PHI at the Florida facilities where they were treated, and Ascension maintained their information on computer systems within the state. In today's digital age, the Court rejects the notion that the presence of that information on Ascension's servers in Missouri would foreclose

the Florida Plaintiffs' home state claims.<sup>12</sup>

Ascension's motion to dismiss will be denied as to this Count IX.

Illinois Statutory Claims (Counts X & XI)

Plaintiffs Angel Negron and Mattie Boyden, on behalf of the Illinois subclass, assert claims under the Illinois Personal Information Protection Act (IPIPA), 815 Ill. Comp. Stat. § 530 (Count X), and the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA), 815 Ill. Comp. Stat. § 505 (Count XI).

On Count X, IPIPA requires any data collector to provide expedient notice of a data breach. § 530/10. Plaintiffs allege that Ascension failed to provide timely and accurate notice of this breach. In support of its motion to dismiss, Ascension contends that IPIPA doesn't create a private right of action. "The only way to pursue a claim under PIPA is by satisfying ICFA's requirements because PIPA does not create a separate cause of action." *SuperValu II*, 925 F.3d at 964. However, where a plaintiff successfully pleads an ICFA claim, the IPIPA claim also survives. *In re Fortra File Transfer Software Data Sec. Breach Litig.*, 749 F. Supp. 3d 1240, 1272 n.14 (S.D. Fla. 2024).

Ascension also argues that Plaintiffs have not plausibly pleaded that it failed to timely notify them of the breach insofar as the complaint itself describes Ascension's immediate response. But what constitutes reasonable and timely notice under the circumstances is a fact

---

<sup>12</sup> This Court does not find persuasive the rationale of *Bellwether Cmty. Credit Union v. Chipotle Mexican Grill, Inc.*, 353 F. Supp. 3d 1070 (D. Colo. 2018), where the court construed venue pleadings to foreclose FDUTPA claims for Florida victims of a Colorado company's data breach because "claims can only substantially occur in one place." *Id.* at 1093. Venue is an entirely separate inquiry, and litigants routinely plead alternate theories on any number of issues. This Court has no trouble accepting that venue is proper in Missouri, where Ascension is domiciled and perhaps certain systemwide decisions were made, and that Florida subclass claims arose in Florida, where Florida Ascension patients received HIPAA Notices, provided their PII/PHI, and suffered losses from the breach.



question beyond the Court's examination of the pleadings at this stage.<sup>13</sup> Plaintiffs can maintain their IPIPA claim if their ICFA claim is viable, which it is.

On Count XI, ICFA prohibits unfair or deceptive practices, including misrepresentation or the concealment or omission of material fact with the intent that others rely on it. § 505/2. Plaintiffs plead that Ascension violated ICFA by misrepresenting that it would protect their PII/PHI, failing to maintain adequate security, and concealing its failure. Plaintiff Boyden further pleads that her information was exposed on the dark web. Conduct is deceptive if it is likely to deceive a reasonable consumer and unfair if it is unethical and causes substantial injury.

*Mashallah, Inc. v. W. Bend Mut. Ins. Co.*, 20 F.4th 311, 322 (7th Cir. 2021).

Again, Ascension argues that Plaintiffs fail to specifically plead reliance on an actionable representation or omission and resulting injury. Federal courts apply Rule 9(b) pleading standards to ICFA claims. *Spivey v. Evig LLC*, 2025 WL 1638453, at \*2 (N.D. Ill. June 9, 2025). But, as previously stated, the Court finds the pleadings sufficient overall.

Ascension also argues that, like the FDUTPA, the ICFA provides a right of action only when the conduct occurs in Illinois, so Plaintiffs' venue pleadings defeat the claim. This theory remains unavailing. "There is no single formula or bright-line test for determining whether a transaction occurs within this state." *Jett v. Warrantech Corp.*, 436 F. Supp. 3d 1170, 1180 (S.D. Ill. 2020). Circumstances will vary in every case, but courts consider "the residency of the plaintiff, the location of harm, communications between parties (where sent and where received), and where a company policy is carried out." *Id.* The Illinois subclass Plaintiffs were treated at Ascension facilities in Illinois where they received Ascension's HIPAA Notice, provided their PII/PHI, and suffered loss from the data breach. The Court finds the pleadings sufficient to state

---

<sup>13</sup> The Court likewise rejects this argument challenging similar claims asserted by the Wisconsin and Michigan subclasses (Counts XV and XVI, respectively).

a claim under the ICFA.

Ascension's motion to dismiss will be denied as to Counts X and XI.

Oklahoma Consumer Protection Act (Count XII)

Plaintiff Cheryl Hayes, on behalf of the Oklahoma subclass, asserts a similar state statutory claim under the Oklahoma Consumer Protection Act (OCPA), Okla. Stat. tit. 15 § 751, *et seq.*<sup>14</sup> Notably, however, OCPA contains an exemption for “actions or transactions” regulated under laws administered by any regulatory body acting under statutory authority. § 754.2. In support of its motion to dismiss on this count, Ascension centrally argues that this exemption precludes Plaintiff Hayes's OCPA claim because Ascension's privacy practices are regulated by HIPAA.

In response, Plaintiffs cite *Robinson v. Sunshine Homes, Inc.*, where the court declined to apply the exemption because the state regulatory framework mainly governed licensing and didn't create a private right of action. 291 P.3d 628, 635 (Okla. Civ. App. 2010). Plaintiffs thus argue that this exemption doesn't apply here because HIPAA provides no monetary redress.

More recently, however, in a case for money damages, the Oklahoma Supreme Court has clearly instructed that “the focus on whether a § 754 exemption applies is determined by whether the action or transaction is regulated and not specifically on whether such regulations also

---

<sup>14</sup> Specifically, Plaintiffs invoke OCPA provisions prohibiting false representations “as to the characteristics, ingredients, uses, benefits, alterations, or quantities of the subject of a consumer transaction or a false representation as to the sponsorship, approval, status, affiliation or connection of a person therewith” and representations “that the subject of a consumer transaction is of a particular standard, style or model, if it is of another.” § 753(5) and (8). Though not briefed by either party, it is unclear to the Court how Ascension's HIPAA notice can be construed to contain representations regarding the “subject of the consumer transaction,” which is health care, not data privacy. These provisions of OCPA don't seem to apply here. However, other provisions of OCPA prohibit deceptive or unfair trade practices in the form of misrepresentations or omissions that could be expected to deceive or mislead a person and cause injury. §§ 752.13 and 14, § 753.21. While Plaintiffs don't expressly invoke these subsections, the complaint sufficiently pleads such practices.

provide a private right of action.” *U.S. Bank Nat’l Ass’n v. Hill*, 540 P.3d 1, 11 (Okla. 2023). Consistent with this view, multiple federal courts have concluded that the OCPA exemption applies regardless of whether a private right of action exists. *Mednax*, a data breach case involving HIPAA violations, is squarely on point. There, the court reasoned that the “actions” in question were those taken by Mednax in the course of safeguarding or failing to safeguard the plaintiffs’ PHI – “actions that fall squarely within the scope of HIPAA.” *Mednax*, 603 F. Supp. 3d at 1217. *See also Gray v. Acadia Healthcare Co., Inc.*, 2020 WL 5996418, at \*11 (E.D. Okla. Oct. 9, 2020) (involving misconduct at a hospital regulated by the Oklahoma department of health); *Sweeny v. Toyota Motor Sales, U.S.A., Inc.*, 2023 WL 2628697, at \*14 (C.D. Cal. Feb. 9, 2023) (reasoning that the Oklahoma motor vehicle commission’s administrative code prohibited false or misleading advertising).

Guided by these cases, the Court will grant Ascension’s motion to dismiss on Count XII.

Wisconsin Statutory Claims (Counts XIII-XV)

Plaintiff Jill Radley, on behalf of the Wisconsin subclass, asserts state statutory claims for breach of confidentiality of patient health care records pursuant to Wis. Stat. § 146.81, *et seq.* (Count XIII), violation of the Wisconsin Deceptive Trade Practices Act (WDTPA), Wis. Stat. § 100.18, *et seq.* (Count XIV), and failure to provide adequate notice of the unauthorized acquisition of personal information, in violation of Wis. Stat. § 134.98(2), *et seq.* (Count XV).

On Count XIII, §§ 146.82 and 83 provide standards similar to HIPAA for the confidentiality and limited release of patient health care records. Section 146.84(1) creates a private right of action for the knowing and willful or negligent release of records in violation of those standards, though no liability attaches when the custodian acts in good faith. In support of its motion to dismiss this count, Ascension argues that the statute doesn’t apply to the present

facts because Ascension didn't release or disclose Plaintiffs' information at all; it was stolen by cybercriminals. While this is a logical reading of the statute's active verbs, two district courts in Wisconsin have rejected this argument in other data breach cases. *Dusterhoft v. OneTouchPoint Corp.*, 2024 WL 4263762, at \*16 (E.D. Wis. Sept. 23, 2024); *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 796 (W.D. Wis. 2019). The Court declines to depart from these Wisconsin decisions and will deny Ascension's motion on Count XIII.

On Count XIV, claims arising under the WDTPA have three elements: "(1) the defendant made a representation to the public with the intent to induce an obligation, (2) the representation was untrue, deceptive or misleading, and (3) the representation materially induced (caused) a pecuniary loss to the plaintiff." *Giasson v. MRA - Mgmt. Ass'n, Inc.*, 2025 WL 1025173, at \*18 (E.D. Wis. Apr. 7, 2025). Notably, the WDTPA applies only to affirmative assertions; an omission is insufficient. *Id.* In support of its motion to dismiss this count, Ascension again contends that Plaintiffs have failed to satisfy Rule 9(b) pleading standards or plausibly allege reliance on an actionable misrepresentation causing injury, and that Ascension's alleged concealment of its inadequate data security doesn't give rise to a WDTPA claim.

Wisconsin courts are split as to whether Rule 9(b) standards apply to WDTPA claims. *See Id.* at \*18 n.13; *Green v. Olympus Grp., Inc.*, 2025 WL 1201995, at \*3 (E.D. Wis. Apr. 25, 2025). And reasonable reliance is not an element but may be considered by the fact finder. *Blitz v. Monsanto Co.*, 317 F. Supp. 3d 1042, 1054 (W.D. Wis. 2018). In any case, Plaintiff Radley pleads that she "reasonably expected that her PII and PHI would remain safe" and that, had she been informed of Ascension's insufficient security, she would not have provided her

information. As for injury, her bank account was compromised, resulting in large withdrawals and unreimbursed overdraft fees. (Doc. 52 at 60). This is sufficient even applying Rule 9(b).

The closer call here is whether Plaintiffs have identified a representation that was “untrue, deceptive, or misleading” for purposes of the WDTPA. Plaintiffs don’t address this count at all in their responsive brief but confirm that their theory of the case – the specific “what” of their complaint – is that Ascension omitted and concealed the fact that its data security practices were inadequate. (Doc. 64 at 38-39). Unlike in other states, this alleged omission doesn’t give rise to a WDTPA claim. *Giasson*, 2025 WL 1025173, at \*18. Rather, the WDTPA requires an active misrepresentation. In *Giasson*, the defendant’s privacy policy represented that it used “reasonable and appropriate” and “industry-standard” security measures to protect PII. The court found this sufficient to constitute an alleged misrepresentation. *Id.*, at 19. In *Dusterhoft*, the defendant’s website stated that it “maintain[ed] commercially reasonable security measures” to protect private information from unauthorized access. 2024 WL 4263762, at \*16. Here, Ascension’s HIPAA Notice merely states that Ascension is “committed to maintaining the privacy and confidentiality of your health information” and “required by law” to do so. (Doc. 52 at 10; Doc. 73-1). In other contexts, such a general statement would not be actionable. *Bakery Bling v. Matrix Packaging Mach., LLC*, 685 F. Supp. 3d 718, 752 (E.D. Wis. 2023) (involving commercial representations). The Court notes that the briefing on this issue is minimal. Out of caution, and given the expectations inherent in HIPAA, the Court will accept Plaintiffs’ pleadings of active misrepresentation at this early stage. *See Dusterhoft*, 2024 WL 4263762, at \*16 (reasoning that whether statements are misleading is a fact question).

On Count XV, § 134.98 requires companies doing business in the state to notify customers within 45 days after any data breach. It states, “Failure to comply with this section is

not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty.” § 134.98(4). In its motion to dismiss this count, Ascension argues that the statute doesn’t create a separate right of action. Ascension cites *Fox*, where the Western District of Wisconsin dismissed a similar claim because “the legislature has not provided any indication that § 134.98 creates a separate right of action.” 399 F. Supp. 3d at 800. Although Plaintiffs cite contrary conclusions from other districts,<sup>15</sup> this Court elects to follow the Wisconsin district court’s interpretation of Wisconsin state law, which aligns with Wisconsin Supreme Court instruction that “courts may not find a statutory right in legislative silence alone.” *Crown Castle USA, Inc. v. Orion Const. Grp., LLC*, 811 N.W.2d 332, 342 (Wis. 2012). Consistent with *Fox*, the Court will dismiss this count as an independent claim, but Plaintiffs may invoke the statute as relevant to their negligence claims.

Ascension’s motion to dismiss will be denied as to Counts XIII and XIV and granted as to Count XV.

Michigan Statutory Claims (Counts XVI-XVII)

Plaintiff Leah Willis, on behalf of the Michigan subclass, asserts claims under the Michigan Identity Theft Protection Act (MITPA), Mich. Comp. Laws § 445.61, *et seq.* (Count XVI) and the Michigan Consumer Protection Act (MCPA), Mich Comp. Laws § 445.901, *et seq.* (Count XVII).

Regarding Count XVI, MITPA § 445.72 requires businesses to give consumers notice of data security breaches “without unreasonable delay.” § 445.72(4). In support of its motion to dismiss this count, Ascension submits that MITPA doesn’t provide an independent right of

---

<sup>15</sup> See *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1341 (N.D. Ga. 2019) (reasoning that the statute is silent on enforcement); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1170 (D. Minn. 2014) (same).

action. Plaintiffs dispute this interpretation but alternatively reserve the right to invoke MITPA through the MCPA.

MITPA creates a misdemeanor for fraudulent notices and empowers the attorney general or a prosecuting attorney to bring civil enforcement actions to recover fines for any violation of the statute. § 445.72(12) and (13). It also clarifies that state enforcement mechanisms “do not affect the availability of any civil remedy for a violation of state or federal law.” § 445.72(15). Some courts have interpreted this to mean that consumers may enforce MITPA § 445.72 through the MCPA. *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1306-7 (S.D. Cal. 2020); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1339 (N.D. Ga. 2019); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014).

However, shortly after the instant motion was fully briefed, the Eastern District of Michigan concluded that a MITPA notice violation (§ 445.72(4)) cannot proceed as an MCPA claim. The MCPA expressly creates a right of action for a different section of MITPA (i.e., § 445.71 prohibiting the denial of credit to a victim of identity theft) but not for the data breach notice section at issue here (§ 445.72). *Angus v. Flagstar Bank, FSB*, 2025 WL 937760, at \*7 (E.D. Mich. Mar. 27, 2025) (citing MCPA § 445.903(1)(jj)). Following the rule of statutory construction *expressio unius est exclusio alterius* – the expression of one thing is the exclusion of another – the court reasoned, “By listing a violation of [§ 445.71] and omitting a violation of [§ 445.72], the Michigan Legislature made clear that a violation of [§ 445.72] is not actionable under the MCPA.” *Id.*

Faced with a conflict between older cases outside the Seventh Circuit and a recent Michigan case interpreting Michigan state law, this Court will follow the thoughtful rationale of

the Michigan district court. *Target* cursorily inferred a MITPA notice cause of action through the MCPA without examining § 445.903(1)(jj), and *Equifax* and *Solara* simply followed *Target*. Only *Angus* provides a meaningful analysis, which this Court finds persuasive. The Michigan legislature clearly knew how to provide relief for a MITPA violation through the MCPA but chose not to do so for the notice provisions. Thus, the Court agrees that MITPA § 445.72 doesn't create a private right of action and also concludes, following *Angus*, that "the MCPA does not authorize a plaintiff to bring a claim based upon a violation of [§ 445.72]." *Id.*

On Count XVII, the MCPA prohibits unlawful trade practices including representations of fact "material to the transaction such that a person reasonably believes the ... state of affairs to be other than it actually is" and "failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner." § 445.903(bb) and (cc). Plaintiffs plead that Ascension misrepresented that it would protect PII/PHI and concealed the fact that its data systems were not secure.

In support of its motion to dismiss this count, Ascension asserts its global arguments that the complaint falls short of Rule 9(b) standards and fails to plead reliance and resulting injury. As previously stated, the Court finds the complaint sufficient in these respects. Plaintiff Willis pleads that she received Ascension's HIPAA Notice and reasonably expected that her PII and PHI would be safe. Had she known of Ascension's inadequate data security, she wouldn't have provided it. Additionally, her surgery was postponed as a result of the breach, leaving her in pain until it could be rescheduled. The Court finds these pleadings sufficient to state an MCPA claim.

Ascension's motion to dismiss will be granted as to Count XVI and denied as to Count XVII.



Indiana Deceptive Consumer Sales Act (Count XVIII)

Finally, Plaintiffs Donald Pitchers and George Gounaris, on behalf of the Indiana subclass, assert a claim under the Indiana Deceptive Consumer Sales Act (IDCSA), Ind. Code §§ 24-5-0.5-3. The IDCSA prohibits unfair or deceptive acts, omissions, or practices in connection with a consumer transaction, including implicit and explicit misrepresentations that occur before, during, or after the transaction. *Reger v. Arizona RV Centers, LLC*, 515 F. Supp. 3d 915, 938 (N.D. Ind. 2021). In support of its motion to dismiss this count, Ascension again asserts its global theories that Plaintiffs have not sufficiently pleaded their reliance on an actionable misrepresentation or omission that caused injury. (Doc. 60 at 40-42).

Indiana courts apply Rule 9(b) pleading standards to IDCSA claims. *Williams v. Thor Motor Coach, Inc.*, 2024 WL 4524292, at \*2 (N.D. Ind. Oct. 17, 2024). Even so, the Court finds the pleadings sufficient to state an IDCSA claim. Plaintiffs plead that, in the course of treatment (the “when and where”), Ascension misrepresented through its HIPAA notice (the “how”) that it would maintain adequate security and comply with privacy laws while knowing that its practices were inadequate, deliberately misleading patients to transact for their health care services (the “what”). (Doc. 52 at 114-15). They plead reliance by alleging that they received Ascension’s Notice and reasonably expected their PII/PHI to remain safe (*Id.* at 54, 56), and had they known of Ascension’s insufficient security, they wouldn’t have provided their information (*Id.* at 55, 57). As for injury, they plead that, a result of the data breach, their information appeared on the dark web, and Pitchers was unable to obtain his medication on time. (*Id.* at 54-55).

These allegations satisfy Rule 9(b) standards for an IDCSA claim. *See e.g., Moore v. Soc. Coaching-Credit Repair, LLC*, 2024 WL 1929431, at \*3 (N.D. Ind. May 1, 2024) (finding IDCSA pleadings sufficient). The Court will deny Ascension’s motion on this Count XVIII.

## CONCLUSION

Accordingly,

**IT IS HEREBY ORDERED** that Defendants' motion to dismiss (Doc. 59) is **GRANTED** with respect to Counts III, IV, V, VI, VII, XII, XV, and XVI and **DENIED** with respect to Counts I, VIII, IX, X, XI, XIII, XIV, XVII, and XVIII.

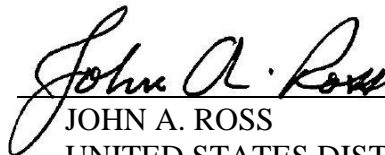
**IT IS FURTHER ORDERED** that, as to Count II, the motion is **GRANTED** as to the FTCA and **DENIED** as to HIPAA.

**IT IS FURTHER ORDERED** that, as to the claims of Plaintiff Tiffany Farrand, the motion is **GRANTED** in its entirety and without prejudice.

**IT IS FINALLY ORDERED** that Defendants' motion to dismiss Ascension Health Alliance and Ascension Technologies is **DENIED** at this time.

An order requiring the parties to submit a joint proposed scheduling plan will issue separately.

Dated this 23rd day of September 2025.

  
\_\_\_\_\_  
JOHN A. ROSS  
UNITED STATES DISTRICT JUDGE