

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
LOUISVILLE DIVISION

JAKETRIUS LURRY, individually and on
behalf of all others similarly situated,

Plaintiffs

v.

Civil Action Lead Case No. 3:23-cv-297-RGJ

PHARMERICA CORPORATION,

Defendant

* * * * *

MEMORANDUM OPINION AND ORDER

This case comes before the Court on Defendant PharMerica Corporation’s (“PharMerica”) motion to dismiss Plaintiffs’ First Amended Consolidated Class Action Complaint. [DE 39]. Briefing is complete and the motion is ripe. For the reasons stated below, PharMerica’s motion to dismiss [DE 39] is **GRANTED in part** and **DENIED in part**.

BACKGROUND

PharMerica is a pharmacy services provider for various healthcare facilities and programs nationwide. [DE 38, First Am. Consolidated Class Action Compl., at 506]. PharMerica collects and maintains personal identifiable information (“PII”) and protected health information (“PHI”) (collectively, “personal information”) of its clients’ patients and employees. [*Id.* at 507]. The entity is incorporated in Delaware with its principal place of business in Louisville, Kentucky. [*Id.* at 513].

Plaintiffs allege that on or around March 2023, a ransomware group known as “Money Message” targeted and breached PharMerica’s computer network, resulting in the exfiltration of

4.7 terabytes of information.¹ [*Id.*]. Plaintiffs allege their personal information was stolen and published online, resulting in ongoing harm. [*Id.*]. PharMerica later distributed HIPPA-required data breach notification letters to the affected parties, including Plaintiffs. [*Id.* at 518–19; DE 39 at 618].

Plaintiffs have various relationships to PharMerica:

1. David Hibbard (“Hibbard”) is a citizen of Kentucky. [DE 38 at 512]. He was employed at ResCare, which subsequently changed its name to BrightSpring and eventually merged with PharMerica. [*Id.* at 547]. He believes he provided his personal information to BrightSpring, which then transferred it to PharMerica as a condition of employment. [*Id.* at 548].
2. Frank Raney (“Raney”) is a citizen of Texas. [*Id.* at 512]. He received services from PharMerica while being treated post-operation at a nursing home. [*Id.* at 550]. He believes he provided his personal information directly to PharMerica as a condition of receiving services. [*Id.*]
3. Holly Williams (“Williams”) is a citizen of South Carolina. [*Id.* at 512]. She has no known relationship to PharMerica. [*Id.* at 522]. She received notice that her information was compromised in the data breach from BrightSpring. [*Id.*].
4. James Young (“Young”) is a citizen of Michigan. [*Id.* at 513]. He has no known relationship to PharMerica. [*Id.* at 554]. He received a letter from PharMerica notifying him that his personal information had been compromised in the data leak. [*Id.*].

¹ According to the amended complaint, “Money Message employs a ‘double extortion’ technique in which it both steals sensitive data from the target’s network and encrypts it so that the target can no longer use the data itself.” It also maintains a “leak site” where the stolen data is posted if a ransom is not paid. [*Id.* at 515].

5. Micaela Molina (“Molina”) is a citizen of California. [*Id.* at 513]. She was employed at BrightSpring—which merged with PharMerica in 2019—from 2021 to 2023. [*Id.* at 555]. She provided her personal information to PharMerica as a condition of employment. [*Id.*].
6. Charley Luther (“Luther”) is a citizen of California. [*Id.* at 513]. She has no known direct relationship to PharMerica. [*Id.* at 557]. She believes that some her personal information was likely transferred from her medical providers to PharMerica during treatment. [*Id.*]

Plaintiffs bring claims on behalf of themselves and all others similarly situated. They seek to certify a Nationwide Class and five state subclasses: Kentucky, California, Michigan, Texas, South Carolina (collectively, “State Subclasses”) (collectively with Nationwide Class, “Class”). [*Id.* at 559–60]. No class has been certified at this time.

STANDARD

Federal Rule of Civil Procedure 12(b)(6) instructs that a court must dismiss a complaint if the complaint “fail[s] to state a claim upon which relief can be granted[.]” Fed. R. Civ. P. 12(b)(6). To state a claim, a complaint must contain “a short and plain statement of the claim showing that the pleader is entitled to relief[.]” Fed. R. Civ. P. 8(a)(2). When considering a motion to dismiss, courts must presume all factual allegations in the complaint to be true and make all reasonable inferences in favor of the non-moving party. *Total Benefits Plan. Agency, Inc. v. Anthem Blue Cross & Blue Shield*, 552 F.3d 430, 434 (6th Cir. 2008) (citation omitted). “But the district court need not accept a bare assertion of legal conclusions.” *Tackett v. M & G Polymers, USA, LLC*, 561 F.3d 478, 488 (6th Cir. 2009) (citation omitted). “A pleading that offers labels and conclusions or a formulaic recitation of the elements of a cause of action will not do. Nor does a complaint suffice

if it tenders naked assertion[s] devoid of further factual enhancement.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation marks and citation omitted).

To survive a motion to dismiss, a plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is 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 (citing *Twombly*, 550 U.S. at 556). “A complaint will be dismissed . . . if no law supports the claims made, if the facts alleged are insufficient to state a claim, or if the face of the complaint presents an insurmountable bar to relief.” *Southfield Educ. Ass’n v. Southfield Bd. of Educ.*, 570 F. App’x 485, 487 (6th Cir. 2014) (citing *Twombly*, 550 U.S. at 561–64).

ANALYSIS

I. Choice of Law

The Amended Complaint alleges six common law claims and six state statutory claims. The statutory claims are brought under the laws of three states: Michigan, Kentucky, and California. The Complaint does not specify under what state law the common law claims are alleged. In its motion to dismiss, PharMerica assumes that Kentucky law applies to the common law claims. Plaintiffs did not object to the application of Kentucky law in their response, and thus likely waived objection to the issue. [*See* DE 40 at 649].

The Sixth Circuit has suggested that courts should evaluate choice of law—but “not delve too deeply” when “all parties have acquiesced[]without comment.” *GBJ Corp. v. E. Ohio Paving Co.*, 139 F.3d 1080, 1085 (6th Cir. 1998). This is because courts “retain[] the independent power to identify and [to] apply the proper construction of governing law” in the dispute. *Kamen v. Kemper Fin. Serv., Inc.*, 500 U.S. 90, 99 (1991).

Thus, the Court will need to engage in the choice of law analysis at some point. At this stage, however, there is insufficient information to engage in a comprehensive choice of law analysis. *See McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810 (E.D. Ky. 2019) (declining to engage in choice of law analysis at the motion to dismiss stage when parties did not fully brief issue). As a result, for this 12(b)(6) motion, the Court will consider the pleaded common law claims—as the parties have done—under the substantive law of Kentucky.

II. Sufficiency of the Complaint

PharMerica moves to dismiss Plaintiffs’ state law claims for negligence, breach of implied contract, breach of third-party beneficiary contract, breach of fiduciary duty, invasion of privacy, unjust enrichment, the Kentucky Consumer Protection Act (“KCPA”), the Michigan Data Breach Prompt Notification law (“MIPTA”), the California Unfair Competition Law (“UCL”), the California Consumer Records Act (“CCRA”), the California Consumer Privacy Act (“CCPA”), and the California Confidentiality of Medical Information Act (“CMIA”). [DE 39 at 623–42].

A. Negligence (Count I)

PharMerica asserts that Plaintiffs fail to state a claim for negligence because they “fail to plead the requisite damages to sustain” their claim. [DE 39 at 623]. “As a general matter, the elements of negligence, familiar to all attorneys and law students, are, (1) that defendant owed the plaintiffs a duty of care, (2) that defendant breached the applicable duty of care, (3) causation, including both cause in fact and proximate cause, and (4) that the plaintiff was damaged by the breach of the duty of care.” *Allconnect*, 369 F. Supp. 3d at 817. The amended complaint alleges multiple damages arising from PharMerica’s negligence, including: “[1] invasion of privacy; [2] theft of and fraudulent use of their Personal Information; [3] lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; [4] loss of

benefit of the bargain; [5] lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; [6] experiencing an increase in spam calls, texts, and/or emails; [7] dissemination of the Personal Information on the dark web; [8] statutory damages; nominal damages; and anxiety, emotional; [9] distress, loss of privacy, and other economic and non-economic losses.” [DE 38 at 569]. Court have routinely upheld these allegations as sufficient to state a claim at the motion to dismiss stage. *See Allconnect*, 369 F. Supp. 3d at 818 (holding monetary and time loss from information safeguarding, emotional distress were sufficient to plead a cognizable injury); *Bowen v. Paxton Media Group, LLC*, No. 5:21-CV-00143-GNS, 2022 WL 4110319, at *6 (W.D. Ky. Sept. 8, 2022) (holding monetary costs, mental distress, and time spent “to address and attempt to ameliorate, mitigate and deal with the actual and future consequences” of a data breach constituted a concrete injury sufficient to survive a motion to dismiss).

PharMerica further argues that Plaintiffs’ claims fail because they are speculative: they fail to identify any “loss or damage arising from the alleged dissemination” of Plaintiffs’ information online. [DE 39 at 625]. It is true that increased risk of future harm is not a stand-alone claim in Kentucky. *See Smith v. Windstream Commc’ns, Inc.*, No. Civ. 11–272–GFVT, 2013 WL 3233488, at *2 (E.D. Ky. June 25, 2013)); *Rainer v. Union Carbide Corp.*, 402 F.3d 608, 619 (6th Cir. 2005) (reviewing Kentucky case law and explaining that a cause of action does not develop until actual harm is realized). However, “a jury may consider whether Plaintiffs are entitled to compensation for their increased risk of future harm as long as they can show a material risk of concrete harm coupled with any realized injury—which could be emotional harm, lost out-of-pocket expenses, or ‘some other injury.’” *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-186-CHB, 2023 WL 2755305, at *15 (W.D. Ky. Mar. 31, 2023) (quoting *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2211 (2021)); *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 388 (6th Cir. 2016)

(“Plaintiffs’ allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation.”); *but see Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205, 2012 WL 2873892, at *8 (W.D. Ky. July 12, 2012) (previously holding “Kentucky courts would not condone payments for credit monitoring unless Plaintiffs’ identities were actually stolen and then used to their financial detriment”).² Thus, at this stage, Plaintiffs may properly claim damages arising from an increased risk of future harm because they have also claimed realized injuries in the form of emotional harm and expenses. As a result, PharMerica’s motion to dismiss Plaintiffs’ negligence claim is denied.

B. Breach of Implied Contract³ (Count II)

PharMerica argues that Plaintiffs have not sufficiently pleaded an agreement between the parties because two Plaintiffs claim to have no relationship with PharMerica, and the others fail to point to any promise of cybersecurity. [DE 39 at 627].⁴ Plaintiffs assert that they need not allege an explicit promise of cybersecurity. [DE 40 at 655].

To establish breach of an implied contract, a Plaintiff must prove the existence of an implied contract, created by mutual assent, and the failure of a party to comply with the contract’s terms. *See Furtula v. University of Kentucky*, 438 S.W.3d 303, 308-09 (Ky. 2014).

² PharMerica cites an earlier decision in *Savidge* to support its claims. [DE 39 at 625]. It fails to note that the Court later revised its holding, stating “[t]he Court is now convinced that it erred, in part, in reaching this conclusion.” *Savidge v. Pharm-Save, Inc.*, No. 3:17-CV-186-CHB, 2023 WL 2755305, at *15 (W.D. Ky. Mar. 31, 2023) (holding, instead “so long as Plaintiffs can show they are at a material risk of concrete harm, and that they have suffered any other harm from that risk—not, as the Court previously held, out-of-pocket expenses specifically—they may be entitled to damages for an increased risk of future harm”).

³ This and Plaintiffs’ breach of third-party beneficiary contract claim are pleaded in the alternative to the unjust enrichment claim. [DE 38 at 570, 573].

⁴ PharMerica also argues that Plaintiffs have failed to allege actual damages. [DE 39 at 628]. That argument fails for the reasons already stated above. *See supra* Part II.A.

Plaintiffs’ relationships with PharMerica vary in nature. Plaintiffs Williams and Young, allege they have “no known relationship with PharMerica” and have “never consented to PharMerica collecting and storing” their personal information. This belies a plausible inference of mutual assent. Similarly, Plaintiff Luther claims to have never provided her information to PharMerica. [DE 38 at 557]. Instead, she alleges her medical providers disclosed her personal information to PharMerica without her knowledge. [*Id.*]. Luther’s allegations likewise do not support an inference of mutual assent, as Luther was unaware of the disclosure. Thus, as to Williams, Young, and Luther, PharMerica’s motion to dismiss is granted.

Plaintiffs Molina and Hibbard provided their personal information to PharMerica as a condition of employment.⁵ [DE 38 at 548, 555]. Similarly, Plaintiff Raney’s personal information was disclosed to PharMerica by the nursing home at which he received post-operation care. The amended complaint alleges his information was provided “as a condition of receiving services from [PharMerica].” [*Id.*]. Such disclosures have repeatedly been found sufficient to state a breach of implied contract claim in data breach cases. *See Allconnect*, 369 F. Supp. 3d at 821 (holding employees who disclosed personal information as a condition of employment stated a claim for breach of implied contract sufficient to survive a motion to dismiss); *Bowen*, 2022 WL 4110319, at *7 (same).

Notably, this case is distinguishable from the breach at issue in *McKenzie* because it involved a breach by third-party ransomware hackers, not one caused by an internal actor “falling prey to a phishing email.” *McKenzie*, 369 F. Supp. 3d at 821. However, courts have also refused to dismiss breach of implied contract claims in cases involving ransomware attacks. *See Hummel*

⁵ Hibbard was employed at ResCare from 2014 to 2020. [DE 38 at 547]. Molina was employed at BrightSpring from 2021 to March 2023. [*Id.* at 555]. The amended complaint asserts that ResCare changed its name to BrightSpring in 2018 and merged with PharMerica in 2019. [*Id.* at 547].

v. Teijin Auto. Techs., Inc., No. 23-CV-10341, 2023 WL 6149059 (E.D. Mich. Sept. 20, 2023) (denying motion to dismiss breach of implied contract claim when cyberattack on an employer compromised employee’s PII because “it is incredibly difficult to imagine, how, in our day and age of data and identity theft, the mandatory receipt of [PII] would not imply the recipient’s assent to protect the information sufficiently.”) (internal quotation omitted); *Lochridge v. Quality Temp. Services, Inc.*, No. 22-CV-12086, 2023 WL 4303577, at *7 (E.D. Mich. June 30, 2023) (holding, under Michigan law, that staffing agency’s requirement that plaintiff provide their PII as a condition of services was sufficient to plead the existence of an implied contract that the agency would protect the PII); *Foster v. Health Recovery Services, Inc.*, 493 F. Supp. 3d 622, 640 (S.D. Ohio 2020) (holding medical service provider’s requirement that patients provide PII was sufficient to state a claim for breach of implied contract in cyberattack case). This Court joins the majority of courts in this circuit and finds that Plaintiffs Molina, Hibbard, and Raney have stated a claim for breach of implied contract.⁶

C. Breach of Third-Party Beneficiary Contract (Count III)

“Under Kentucky law, . . . for a breach of contract as a stranger to the contract, the party must show that he is an intended third-party beneficiary of that contract.” *Laurel Constr. Co., Inc. v. Paintsville Util. Comm’n.*, 336 S.W.3d 903, 907 (Ky. App. 2010), as modified (May 28, 2010) (quoting *Sexton v. Taylor County*, 692 S.W.2d 808, 810 (Ky. App. 1985)). “Only a third-party who was intended by the parties to benefit from the contract, namely, a donee or a creditor beneficiary, has standing to sue on a contract; an incidental beneficiary does not acquire such right.” *Presnell Constr. Managers, Inc. v. EH Const., LLC*, 134 S.W.3d 575, 579 (Ky. 2004)

⁶ PharMerica also argues that Plaintiffs are attempting to enforce HIPAA and the FTC Act through their implied contract claim. [DE 39 at 628]. Plaintiffs’ claim makes no such reference to a statutory obligation. [DE 38 at 570–72]. Instead, the amended complaint alleges PharMerica “agreed that it was required to reasonably safeguard the Personal Information from unauthorized access or disclosure.” [*Id.* at 571].

(internal quotations and citations omitted). One “is a creditor beneficiary if the promisee’s expressed intent is that the third party is to receive the performance of the contract in satisfaction of any actual or supposed duty or liability of the promisee to the beneficiary.” *Sexton*, 692 S.W.2d at 810.

Viewing the allegations in the light most favorable to Plaintiffs, the Court finds they have failed to plead facts that would support a plausible inference that Plaintiffs were intended third-party beneficiaries to any specific contract. The amended complaint alleges only that PharMerica contracts with “healthcare partners . . . for the benefit of Plaintiffs and the Class.” [DE 38 at 573]. It fails to identify any specific healthcare partner or allege any connection between that partner and one or more of Plaintiffs. Further, even if the Court accepted Plaintiffs’ argument that the receipt of the data breach notice creates a reasonable inference of a contractual relationship, Plaintiffs fail to allege which parties are in privity or their “expressed intent.” [DE 40 at 657]. The Court need not accept such bare assertions “devoid of further factual enhancement.” *Iqbal*, 556 U.S. at 678. Thus, PharMerica’s motion to dismiss is granted as to this claim.

D. Breach of Fiduciary Duty (Count IV)

PharMerica argues that Plaintiffs have failed to plead the existence of a fiduciary relationship. [DE 39 at 630]. Plaintiffs contend that PharMerica owes a fiduciary duty to its employees and its patients. [DE 40 at 658].

A fiduciary relationship is one “founded on trust or confidence reposed by one person in the integrity and fidelity of another and which also necessarily involves an undertaking in which a duty is created in one person to act primarily for another’s benefit in matters connected with such undertaking.” *ATC Distrib. Grp., Inc. v. Whatever It Takes Transmissions & Parts, Inc.*, 402 F.3d

700, 715 (6th Cir. 2005) (quoting *Steelvest, Inc. v. Scansteel Serv. Ctr., Inc.*, 807 S.W.2d 476, 485 (Ky. 1991)).

Plaintiffs point to no case establishing a general fiduciary relationship between employee and employer. Nor could they because courts have rejected the idea that there is an automatic fiduciary relationship. In *Allconnect*, the court held, in the context of a data breach, that Plaintiffs had failed to plead facts establishing a fiduciary relationship as opposed to an average employment relationship. *See Allconnect*, 369 F. Supp. 3d at 823 (citing *Flegles, Inc. v. TruServ Corp.*, 289 S.W.3d 544, 552 (Ky. 2009) (“A fiduciary, moreover, is one who has expressly undertaken to act for the plaintiff’s primary benefit. . . . Although fiduciary relationships can be informal, a fiduciary duty does not arise from the universal business duty to deal fairly nor is it created by a unilateral decision to repose trust and confidence.”). Specifically, the court suggested a plaintiff would need to allege that the employer “expressly undertook, formally or informally, a duty to act for employees’ benefit” in the context of securing their personal information. *Id.* at 823.

Plaintiffs have failed to allege any such representations that PharMerica made to its employees or patients to secure their data. In their response, Plaintiffs point only to the “privacy policy” posted on PharMerica’s website to support their allegation of fiduciary duty. [DE 38 at 514]. However, making all reasonable inferences in Plaintiffs’ favor, the policy neither purports to create a fiduciary relationship; nor does it suggest PharMerica has undertaken any particular duties with respect to data security. [*Id.*]. The policy is also not alleged to be directed solely at patients or employees. Standing alone, it is insufficient to infer the existence of “an undertaking” between the parties “in which a duty is created in one person to act primarily for another’s benefit in matters connected with such undertaking.” *ATC Distrib.*, 402 F.3d at 715 (quoting *Steelvest*, 807 S.W.2d at 485). Other courts have held similarly. *See Tucker v. Marietta Area Health Care*,

Inc., No. 2:22-CV-184, 2023 WL 423504, at *5 (S.D. Ohio Jan. 26, 2023) (holding a HIPAA-required notice of privacy policy did not create any rights or obligations between the parties) (citing cases).

Nor do Plaintiffs provide any Kentucky case law to support their position that all medical providers owe patients an automatic fiduciary duty in regards to medical information. Instead, they cite cases applying Ohio, New York, and Georgia law. *See, e.g., Tucker v. Marietta Area Health Care, Inc.*, No. 2:22-CV-184, 2023 WL 423504 (S.D. Ohio Jan. 26, 2023) (explaining Ohio law recognizes a fiduciary duty to keep patients' medical information confidential). These cases offer no support for Plaintiffs' Kentucky law claim.

In short, Plaintiffs fail to allege sufficient facts from which to infer the existence of a fiduciary relationship between themselves and PharMerica. *See Tackett*, 561 F.3d at 488 (citation omitted) (a court "need not accept a bare assertion of legal conclusions"). Thus, Plaintiffs' breach of fiduciary duty claim is dismissed.

E. Invasion of Privacy (Count V)

In Kentucky invasion of privacy may consist of four distinct torts: (1) unreasonable intrusion upon seclusion; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to one's private life; and (4) publicity that places another in a false light. *Allconnect*, 369 F. Supp. 3d at 819. Only intrusion upon seclusion is at issue. [DE 39 at 631; DE 40 at 659].

Kentucky has adopted the Restatement (Second) of Torts definition. *See Pearce v. Whitenack*, 440 S.W.3d 392, 400 n.5 (Ky. Ct. App. 2014) (citing *McCall v. Courier-J. & Louisville Times Co.*, 623 S.W.2d 882, 887 (Ky. 1981) (adopting Restatement (Second) of Torts § 652A (Am. Law Inst. 1977))). The elements of intrusion upon seclusion are (1) an intentional intrusion

by defendant, (2) into a matter that plaintiff has a right to keep private, and (3) which is highly offensive to a reasonable person. *Id.* at 400-01.

PharMerica argues Plaintiffs have failed to allege that it acted intentionally. [DE 39 at 631–32]. However, “[a] defendant’s actions may be intentional when the Defendant acts with such reckless disregard for the privacy of the plaintiff that the actions rise to the level of being an intentional tort.” *Allconnect*, 369 F. Supp. 3d at 819 (citing *Smith v. Bob Smith Chevrolet, Inc.*, 275 F.Supp.2d 808, 822 (W.D. Ky. 2003)).

Courts have repeatedly held that being aware of the risk of data breaches and failing to implement appropriate policies is sufficient to state a claim for intrusion upon seclusion. *See id.* (refusing to dismiss an intrusion upon seclusion claim when plaintiffs alleged that defendant was aware of phishing scam risks and failed to train its employees); *Savidge*, 2021 WL 3076786 (holding same); *Bowen*, 2022 WL 4110319 (holding plaintiffs adequately pleaded claim of intrusion on seclusion by alleging that defendant knew its information security practices were inadequate). Likewise, Plaintiffs allege PharMerica “knew its information security practices were inadequate” and “failed to properly safeguard Plaintiffs’ and Class Members’ Private Information despite that knowledge.” [DE 38 at 576]. Taken as true, these allegations are sufficient state a claim for intrusion upon seclusion under Kentucky law. PharMerica’s motion to dismiss the claim is denied.

F. Unjust Enrichment (Count VI)

Next, PharMerica argues that Plaintiffs have failed to state a claim for unjust enrichment, and even if they did, such a claim is barred by the economic loss rule. [DE 39 at 632–33]. Plaintiffs argue that they have pleaded all elements of the claim and are free to plead in the alternative at this stage of litigation. [DE 40 at 660].

In Kentucky, to sustain a claim for unjust enrichment a plaintiff must establish three elements: “(1) [a] benefit conferred upon defendant at plaintiff’s expense; (2) a resulting appreciation of benefit by defendant; and (3) inequitable retention of that benefit without payment for its value.” *Superior Steel, Inc. v. Ascent at Roebling’s Bridge, LLC*, 540 S.W.3d 770, 778 (Ky. 2017) (quoting *Furlong Dev. Co. v. Georgetown-Scott Cty. Planning & Zoning Comm’n*, 504 S.W.3d 34, 39–40 (Ky. 2016)). “Kentucky courts have consistently found that the first element not only requires a benefit be conferred upon the defendant, but also that the plaintiff be the party conferring that benefit.” *Simpson v. Champion Petfoods USA, Inc.*, 397 F. Supp. 3d 952, 973 (E.D. Ky. 2019) (citation omitted).

This Court has held that employees may state a claim for unjust enrichment against an employer which fails to safeguard their data from a cyberattack. *See Bowen*, 2022 WL 4110319, at *8; *see also Foster*, 493 F. Supp. 3d 622 (holding patient sufficiently pleaded unjust enrichment by alleging defendant failed to safeguard his PII but retained patient’s payment for medical services). Plaintiffs allege that they have conferred a benefit on PharMerica by paying for healthcare services and by performing labor in connection with employment. [DE 38 at 577]. They also allege that PharMerica “enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs’ and Class Members’ Personal Information.” [*Id.* at 578]. Accordingly, Plaintiffs have stated a claim for unjust enrichment.

PharMerica also argues that the economic loss rule bars Plaintiffs’ claim. An unjust enrichment claim cannot stand if premised on the same facts as a breach of contract claim. *Poynter v. Ocwen Loan Servicing, LLC*, No. 3:13-CV-773-DJH-CHL, 2016 WL 5380926, at *6 (W.D. Ky., Sept. 23, 2016). This is known as the economic loss rule. At the motion to dismiss stage, however, this Court has held that when there is a dispute as to the existence of a contractual relationship,

dismissal of certain equitable claims is not proper. *Holley Performance Prod., Inc. v. Keystone Auto. Operations, Inc.*, No. 1:09-CV-00053-TBR, 2009 WL 3613735, at *6 (W.D. Ky., Oct. 29, 2009) (“This case has not advanced so far that the contract has been clearly established by the Court as valid and enforceable. Therefore. . .at this early stage of litigation, it is proper for [the plaintiff] to allege both its claim for breach of contract and unjust enrichment.”). The Court’s role at the motion to dismiss stage is to determine whether all claims are sufficiently pleaded. *See Twombly*, 550 U.S. at 570. Under Fed. R. Civ. P. 8(d)(2), plaintiffs are permitted to plead in the alternative. Thus, the economic loss rule does not bar Plaintiffs’ claim at this time.

G. KCPA (Count VII)

The Kentucky Consumer Protection Act (“KCPA”) prohibits the use of “[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce” and “provides a private remedy to ‘any person who purchases or leases goods or services primarily for personal family or household purposes and thereby suffers any ascertainable loss of money or property as a result of’ a violation of [KRS §] 367.170.” Ky. Rev. Stat. § 367.170(1); *Ky Laborers Dist. Council Health & Welfare Tr. Fund v. Hill & Knowlton, Inc.*, 24 F. Supp. 2d 755, 772 (W.D. Ky. 1998) (quoting Ky. Rev. Stat. § 367.220). To assert a KCPA claim, a plaintiff must allege that defendant engaged in “[u]nfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce” and that such practices caused plaintiff’s harm. Ky. Rev. Stat. § 367.170(1). “[T]he plain meaning of the KCPA damages provision requires only a showing of a causal nexus between the plaintiff’s loss and the defendant’s allegedly deceitful practice, not a strict showing that the plaintiff relied on the defendant’s allegedly deceitful practice.” *M.T. v. Saum*, 7 F. Supp. 3d 701, 706 (W.D. Ky. 2014) (quoting *Corder v. Ford Motor Co.*, 869 F.Supp.2d 835, 838 (W.D. Ky. 2012)).

First, PharMerica argues that employees cannot bring KCPA claims against an employer because they do not qualify as one “who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money or property[.]” KRS § 367.220. This court has held as much. *See Bowen*, 2022 WL 4110319, at *10 (dismissing KCPA claim brought by employees against employer because employees are not consumers). Thus, the claim must be dismissed as to the Hibbard and Molina.

Further, PharMerica argues that no named plaintiff has suffered an “ascertainable loss.” [DE 39 at 634]. Plaintiffs argue that they are not required to allege a specific amount of damages, and even if they were, they have alleged damages in the form of fraudulent credit card charges and the cost of additional credit monitoring services.⁷ [DE 40 at 662].

An “ascertainable loss” can be shown by “actual damages” incurred as out-of-pocket expenses or by proof that the customer “purchased an item that is different from or inferior to that for which he bargained[.]” *Complete Auto. Repair Services v. Capps*, No. 2012-CA-002145-MR, 2015 WL 2445911, *5 (Ky. App. May 22, 2015), as modified (May 29, 2015). In the end, the Court need not decide whether any of Plaintiffs’ allegations amount to actual damages because Plaintiffs’ claim suffers from a different fatal defect: it lacks “a causal nexus between the plaintiff[s’] loss and the defendant’s allegedly deceitful practice.” *Saum*, 7 F. Supp. 3d at 706 (quoting *Corder*, 869 F.Supp.2d at 838).

This Court recently considered this issue in an analogous case. *See Cole v. Mariner Fin., LLC*, 673 F. Supp. 3d 867 (W.D. Ky. 2023), appeal dismissed, No. 23-5569, 2023 WL 6142349 (6th Cir. Sept. 5, 2023). In *Cole*, a woman brought a KCPA claim against a lender after she alleged it mailed her a high-interest loan solicitation containing a “live check.” *Id.* at 868. She alleged

⁷ The only Plaintiff who alleges specific actual damages is Hibbard, who was a PharMerica employee.

someone stole her mail, cashed the check, and thereby stole her identity. *Id.* In considering a motion to dismiss, the Court reasoned plaintiff had failed to establish the necessary causal nexus to show an ascertainable loss because her injuries were predicated on the actions of a third party, not on defendant's mailing of the check. *Id.* at 872.

This case is analogous to *Cole*. PharMerica provided services, which Plaintiffs allege created an implied contract for the storage and protection of their personal information. PharMerica then stored that information, albeit in an allegedly negligent manner. Money Message—a third party—then hacked PharMerica's systems, stole Plaintiffs' personal information, and published it, causing Plaintiffs to incur damages. PharMerica's allegedly insufficient cybersecurity policies are analogous to the lender's choice to mail customers live checks in *Cole*. The policies, standing alone, did not proximately cause each plaintiff's injuries: their personal information would not have been disclosed absent the actions of a third party. Thus, Plaintiffs fail to allege a causal nexus between PharMerica's actions and Plaintiffs' alleged injuries—a necessary element of a KCPA claim.

In response, Plaintiffs cite a New Jersey case which held that data breach plaintiffs' KCPA claims survived a motion to dismiss. *In re Am. Med. Collection Agency, Inc. Cust. Data Sec. Breach Litig.*, No. CV 19-MD-2904, 2023 WL 8540911, at *9 (D.N.J. May 5, 2023) (“AMCA”). The case does not control here for two reasons. First, this Court is not bound by a New Jersey court's holding on Kentucky law. *See Mid-Century Ins. Co. v. Fish*, 749 F. Supp. 2d 657, 667 (W.D. Mich. 2010) (“[A] federal court's interpretation of state law is not binding.” (emphasis omitted)). Second, the court in *AMCA* held that plaintiff had alleged sufficient damages in a one-sentence footnote:

The Court also notes that is not convinced that these statutes limit ascertainable loss such that the harms identified supra . . . would be insufficient to establish damages.

See . . . Complete Auto. Repair Servs. v. Capps, No. 2012-CA-002145-MR, 2015 WL 2445911, at *5 (Ky. Ct. App. May 22, 2015), as modified (May 29, 2015) (concluding that “a person is not required to allege a specific amount of actual damages that he has already incurred as out-of-pocket expenses to make out a prima facie case under” the KCPA).

Id. at *9 n. 26. The court did not consider whether plaintiffs had alleged a causal nexus, as required under Kentucky law. *See Corder*, 869 F.Supp.2d at 838 (“[T]he plain meaning of the KCPA damages provision requires only a showing of a causal nexus between the plaintiff’s loss and the defendant’s allegedly deceitful practice, not a strict showing that the plaintiff relied on the defendant’s allegedly deceitful practice.”). Thus, Plaintiffs’ citation is unpersuasive here. Because Plaintiffs have failed to allege PharMerica’s allegedly violative conduct caused an ascertainable loss, PharMerica’s motion to dismiss this claim is granted.

H. MIPTA (Count VIII)

Michigan subclass representative Young alleges claims under the Michigan Identity Theft Protection Act (“MITPA”) on behalf of himself and the state subclass.

MITPA requires businesses to provide notice of a security breach, “without unreasonable delay” to a Michigan resident if that resident’s unencrypted and unredacted “personal information” was accessed by an unauthorized person. Mich. Comp. Laws § 445.72(1). “Personal information” is defined as a person’s “first name or first initial and last name” linked to one or more data elements including a “credit or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident’s financial accounts.” *Id.* § 445.63(r). The MITPA notice provision applies when the business discovers a security breach or receives notice of a security breach unless the breach is not likely to cause harm. *Id.* § 445.7

PharMerica argues that Young’s claim should be dismissed because MIPTA does not create a private right of action. [DE 39 at 634]. The “attorney general or a prosecuting attorney

may bring an action to recover” a civil fine for violating the statute. Mich. Comp. Laws § 445.72(13). However, the statute also provides that “Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law.” *Id.* § 445.72(15). Courts have held this “implies that consumers may bring a civil action to enforce Michigan’s data-breach notice statute through Michigan’s consumer-protection statute or other laws,” and thus private claims brought under another state law should not be dismissed because of a lack of a private right of action. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014); *see also In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1339 (N.D. Ga. 2019) (declining to dismiss MITPA claim because private citizens may enforce the notification statute through other laws); *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1306–07 (S.D. Cal. 2020) (holding same). Unlike the cited cases, Plaintiffs here fail to allege violation of any other Michigan law. *See In re Target*, 66 F. Supp. 3d at 1169 (alleging a Michigan Consumer Protection Act claim in addition to MITPA claim); *In re Equifax*, 362 F. Supp. 3d at 1339 (same); *In re Solara*, 613 F. Supp. 3d at 1306–07 (same). Thus, Plaintiffs’ standalone MITPA allegation is dismissed with leave to amend.⁸

I. California Law Claims (Counts IX, X, XI, and XII)

1. *Presumption Against Extraterritoriality*

California subclass representatives Molina and Luther allege claims under four California state laws. PharMerica argues, first, that all four claims should be dismissed because California applies a presumption against extraterritoriality. [DE 39 at 636]. Plaintiffs argue that the

⁸ Plaintiffs requested leave to amend their Amended Complaint to add a MITPA claim. [DE 40 at 663]. PharMerica did not object to the request in its reply. [See DE 43]. Plaintiffs’ request is both narrow and specific. *C.f. Bey v. WalkerHealthCareIT, LLC*, No. 2:16-CV-01167-GCS, 2017 WL 10992207, at *2 (S.D. Ohio July 25, 2017) (denying plaintiff’s request for leave to amend embedded in a response to a motion to dismiss because she “fail[ed] to define which deficiencies she would cure and offers no explanation of how she would cure said deficiencies”).

presumption does not apply because both Molina and Luther were California residents at all relevant times in the complaint. [DE 40 at 665]. Because the presumption is alleged to bar all California state law claims, the Court addresses it first.

California law presumes that the legislature “did not intend the statutes of th[e] state to have force or operation beyond the boundaries of the state.” *Norwest Mortg., Inc. v. Superior Ct.*, 85 Cal. Rptr. 2d 18, 23 (Cal. App. 4th Dist. 1999) (citation omitted). Unless the legislature explicitly indicates otherwise, “if the liability-creating conduct occurs outside of California, California law generally should not govern that conduct.” *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018). This presumption applies with “full force” to claims under the UCL. *See Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) (“[T]he presumption against extraterritoriality applies to the UCL in full force.”); *McKinnon v. Dollar Thrifty Auto. Grp.*, No. 12-4457 SC, 2013 WL 791457, at *4 (N.D. Cal. Mar. 4, 2013) (“With regard to the UCL and CLRA, non-California residents’ claims are not supported where none of the alleged misconduct or injuries occurred in California.”) (internal quotation marks omitted). Thus, a plaintiff’s residence alone is insufficient to bring claims under the UCL if their injuries took place elsewhere. *McKinnon*, 2013 WL 791457, at *5.

Whether application of the UCL would be impermissible here turns on “whether ‘the conduct *which gives rise to liability* . . . occurs in California.’” *Leibman v. Prupes*, No. 2:14-cv-09003, 2015 WL 3823954, at *7 (C.D. Cal. June 18, 2015) (quoting *Diamond Multimedia Sys., Inc. v. Superior Court*, 968 P.2d 539, 554 (Cal. 1999) (emphasis added)). Two recent cases considering this question inform the Court’s approach.

In *Toretto v. Donnelley Fin. Solutions, Inc.*, a group of plaintiffs brought a UCL claim, among others, after their data was stolen from defendant’s possession. 583 F. Supp. 3d 570, 581

(S.D.N.Y. 2022). The conduct which gave rise to the data breach occurred “entirely outside of California.” *Id.* at 604. Nevertheless, the California plaintiff argued that he could bring a UCL claim because he resided in California and “Defendant’s conduct allegedly caused injury in California.” *Id.* The court rejected this argument, holding that such an application of the UCL would “cause it to operate impermissibly out of state.” *Id.* at 605.

First, the court noted the absence of binding precedent on this question in California. *Id.* at 604–05 (“there is no binding precedent governing whether the UCL applies to a claim by a plaintiff who is a California resident and was allegedly injured in California by out-of-state conduct, but who alleges no connection between the defendant and California”). It then distinguished two lower-court cases on the question: *Norwest*, 85 Cal. Rptr. 2d at 22, and *Yu v. Signet Bank/Virginia*, 82 Cal. Rptr. 2d 304, 313 (1999)). *Norwest* held that Californian plaintiffs could bring UCL claims regardless of where a defendant’s conduct occurred. 85 Cal. Rptr. 2d at 23. *Yu* similarly held that for a defendant to be liable for out-of-state conduct under the UCL, the conduct must “injure a California resident” and “the defendant be subject to jurisdiction in California.” *Toretto*, 583 F. Supp. 3d at 605 (citing *Yu*, 82 Cal. Rptr. 2d at 313.) The cases were distinguishable, per the court, because the plaintiff in *Toretto*, unlike those in *Yu* and *Northwest*, had alleged no facts linking defendant to California. *Id.* The court held that the California Supreme Court would not likely read *Yu* and *Northwest* so broadly as to apply to a defendant whose conduct occurred wholly outside the state. *Id.* Thus, plaintiff’s UCL claim was dismissed.

In *In re Arthur J. Gallagher Data Breach Litigation*, a court in the Northern District of Illinois came to a similar conclusion about California’s presumption against extraterritoriality. 631 F. Supp. 3d 573 (N.D. Ill. 2022). In that case, California plaintiffs brought UCL claims after their data was stolen in a ransomware attack. *Id.* at 581. To determine whether application of the UCL

would be extraterritorial, the court asked whether the “conduct that creates liability occurs in California.” *Id.* at 596 (quoting *Sullivan v. Oracle Corp.*, 254 P.3d 237, 248 (2011) (internal quotation omitted)). Defendant’s wrongful conduct, namely the implementation of inadequate security procedures, stemmed from its principal place of business in Illinois. *Id.* Thus, the UCL claims were dismissed.

The Court finds both *In Re Arthur* and *Toretto* persuasive. Plaintiffs Molina and Luther were both California residents and allege that they incurred their injuries in California. [DE 40 at 665]. Like the defendants in *In Re Arthur* and *Toretto*, PharMerica is headquartered out of state and all the relevant conduct leading to the data breach, and, presumably, the data breach itself, is alleged to have taken place in Kentucky. *See also Raheel Foods, LLC v. Yum! Brands, Inc.*, No. 3:16-CV-00451-GNS, 2017 WL 217751, at *8 (W.D. Ky. Jan. 18, 2017) (holding defendants’ California contacts were insufficient to support an extraterritorial UCL claim when the allegedly unlawful and unfair conduct “appears to have emanated from outside of California, especially in light of the fact that Defendants’ principal offices are located in Kentucky”); *McKinnon v. Dollar Thrifty Auto. Group, Inc.*, No. 12-4457 SC, 2013 WL 791457, at *5 (N.D. Cal. Mar. 4, 2013) (dismissing UCL claim by California resident when pleadings suggested that her injury arose in Oklahoma, not California).

Plaintiffs argue that nonetheless, PharMerica has extensive contacts in California. [DE 40 at 665]; *c.f. Toretto*, 583 F. Supp. 3d at 605. But they fail to connect those contacts and these Plaintiffs, or even the data breach generally. Thus, the Court dismisses the UCL claims.⁹

⁹ PharMerica moved to dismiss all California state law claims under the presumption against extraterritoriality. However, it cites only to cases applying the presumption to UCL claims. It cites no law to support the dismissal of Plaintiffs’ other California claims under the principle. In fact, many of the cases the Court cites dismissed UCL claims on extraterritoriality while considering other California law claims on their merits. *See e.g. Toretto*, 583 F. Supp. 3d at 605 (dismissing UCL claim for extraterritoriality while

2. CCRA and CCPA Claims (Counts X, XI)

PharMerica also argues that Plaintiffs have failed to adequately allege claims under both the California Consumer Privacy Act (“CCPA”) and the California Consumer Records Act (“CCRA”) because PharMerica is exempted from the statutes under HIPAA. Plaintiffs do not dispute that the exposure of HIPAA-protected information is excluded but argue that the Court should recognize the exposure of non-medical information as triggering liability. [DE 40 at 667 (citing *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020))].

The Court turns first to the CCPA claim. Another court in this circuit recently rejected the reasoning in *Stasi*, holding that a medical/ non-medical information distinction is not supported by the text of the statute. *Tate v. EyeMed Vision Care, LLC*, No. 1:21-CV-36, 2023 WL 6383467 (S.D. Ohio Sept. 29, 2023) (“*Stasi* failed to consider the fact that subparagraph (B) of § 1798.145(c)(1) exempts ‘provider[s]’ of health care (who are subject to HIPAA) from the statute ‘to the extent the provider . . . maintains patient information in the same manner as medical information.’ (emphasis added).”). The court dismissed the claim because plaintiffs failed to allege that the defendant maintained “non-medical patient information in a different manner than medical information—a fact required to establish the California statute covers [defendant].” *Id.* Plaintiffs here have similarly failed to allege that fact.

Turning to the CCRA claims, PharMerica alleges that the CCRA’s similar language also exempts it from liability. Cal. Civ. Code § 1798.81.5(e)(3) (exempting any “covered entity governed by the medical privacy and security rules issued” under HIPAA). Plaintiffs again cite to *Stasi* for the proposition that medical and non-medical information should be distinguished. [DE

considering CCRA claim under pleading standard); *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d at 592–96 (dismissing UCL claim for extraterritoriality while considering CCPA, CCRA, and CMIA claims under pleading standard). Thus, the Court declines PharMerica’s invitation to expand the presumption to other California statutes.

40 at 667]. However, even if the Court accepted *Stasi*'s reasoning, that case does not address the CCRA's HIPAA exception at all. *See* 501 F. Supp. 3d at 924–25. Plaintiffs cite no other law to support their assertion that PharMerica is liable under the CCRA, even though its HIPAA exclusion is substantially similar to that in the CCPA.¹⁰

Thus, PharMerica's motion to dismiss is granted as to both the CCRA and CCPA claims.

3. CMIA (Count XII)

The California Confidentiality of Medical Information Act ("CMIA") requires health care providers to maintain medical information "in a manner that preserves the confidentiality of the information contained therein" Cal. Civ. Code §§ 56.101(a). The Act can be split into three distinct claims: section 56.10(a) prohibits "disclosure," section 56.101(a) establishes a duty to "preserve confidentiality," and section 56.36(b) allows a private right of action for "negligent release." Plaintiffs allege violations of section 56.10 and 56.101.

PharMerica first argues that the CMIA requires an affirmative act of disclosure by defendant, which Plaintiffs have failed to plead. This is true for violations of section 56.10(a), but not for violations of section 56.101(a). *See Regents of U. of California v. Superior Ct.*, 163 Cal. Rptr. 3d 205, 217 (Cal. App. 2d Dist. 2013), as modified on denial of reh'g (Nov. 13, 2013) ("disclose" under CMIA means an "affirmative act of communication"); *Sutter Health v. Super. Ct.*, 174 Cal. Rptr. 3d 653, 659 (Cal. App. 3d Dist. 2014) ("Thus, disclosure, under section 56.10, subdivision (a) implies an affirmative communicative act."). Section 56.101 instead requires a showing that "negligence result[ed] in unauthorized or wrongful access to the information," i.e.

¹⁰ The Court also notes that neither Molina nor Luther are likely to fall within the CCRA's definition of "customer." The Complaint contains no allegation that either Plaintiff provided their personal information to PharMerica "for the purpose of obtaining a service from the business." Cal. Civ. Code § 1798.80(c). Molina was an employee, not a customer. [DE 38 at 555]. And Luther denies ever having provided her personal information to PharMerica. [*Id.* at 557].

that the information was “improperly viewed or otherwise accessed.” *Stasi*, 501 F. Supp. 3d at 923 (quoting *Regents*, 163 Cal. Rptr. 3d at 208). The allegations in the Complaint do not support an inference that PharMerica affirmatively communicated Plaintiffs’ confidential information. Thus, the CMIA claim is proper only as an allegation under section 56.101.

Next, PharMerica argues that Plaintiffs have not adequately pleaded that there was an “unauthorized viewing” of their medical records, as required under section 56.101. This argument is unavailing. Luther, the only remaining named California Plaintiff, alleged that she received notice that her data was exposed in the breach. [DE 38 at 558]. She also alleged an increase in spam phone calls and text messages since the breach, including one specific instance of attempted fraud involving her PPI. [*Id.* at 558]. Courts have repeatedly held this is sufficient to give rise to an inference that a plaintiff’s information was exposed. *See In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1299 (S.D. Cal. 2020) (holding plaintiffs’ allegations of disclosure letters and increase in “medical-related spam email and phone calls” was sufficient to plead unauthorized viewing); *In re Mednax Services, Inc., Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183 (S.D. Fla. 2022) (holding allegation of an uptick in phishing emails was sufficient to plead unauthorized viewing).

Finally, PharMerica argues that the amended complaint does not allege that Plaintiffs’ disclosed information is of the type covered by the California statute. The CMIA covers only medical information, which is defined as “any individually identifiable information . . . regarding a patient’s medical history, mental health application information, mental or physical condition, or treatment.” Cal. Civ. Code § 56.05. Plaintiff Molina does not specifically allege that any of her medical information was compromised—only her personal information. [DE 38 at 556]. Her name and Social Security number, standing alone, “do not constitute ‘medical information’ as the

statute defines the term.” *Tate*, 2023 WL 6383467, at *9. Thus, she fails to state a claim under the CMIA and PharMerica’s motion to dismiss is granted as to Molina.


Luther, on the other hand, alleges that her medications and health insurance information were disclosed. [DE 38 at 557]. While these allegations are thin, they distinguish this case from those in which the nature of the disclosed information was not sufficiently alleged. *Cf. Wilson v. Rater8, LLC*, No. 20-CV-1515-DMS, 2021 WL 4865930, *5 (S.D. Cal. Oct. 18, 2021) (holding physician names and appointment and discharge dates and times were not “medical information” under CMIA); *Eisenhower Med. Ctr. v. Superior Ct.*, 172 Cal. Rptr. 3d 165, 170 (Cal. App. 4th Dist. 2014) (“the mere fact that a person is or was a patient is not accorded the same level of privacy as more specific information about his medical history”). Thus, PharMerica’s motion to dismiss Luther’s CMIA claim is denied.

CONCLUSION

For these reasons, **IT IS ORDERED** that:

- 1) PharMerica’s motion to dismiss the First Amended Consolidated Class Action Complaint [DE 39] is **GRANTED** as to Counts III, IV, VII, VIII, IX, X, and XI and **DENIED** as to Counts I, II, V, VI, XII;
- 2) Count XII is **DISMISSED** as to Plaintiff Molina.
- 3) Plaintiffs are GRANTED leave to amend the complaint as to their Michigan law claim.

cc: Counsel of Record


 Rebecca Grady Jennings, District Judge
 United States District Court

June 12, 2024