UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JENNIFER HUMMEL,

Plaintiff,

v.

TEIJIN AUTOMOTIVE TECHNOLOGIES, INC.

Defendants.
_____/

Case No. 23-cv-10341

Paul D. Borman
United States District Judge

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS (ECF No. 12)

INTRODUCTION

In this action, Plaintiff Jennifer Hummel, on behalf of a class of similarly situated individuals, asserts claims of negligence, breach of implied contract, and declaratory judgment against her employer, Defendant Teijin Automotive Technologies ("Teijin"). Plaintiff's claims arise from a data breach which occurred when one of Defendant's employees unwittingly clicked on a phishing-email, which gave computer hackers access to the personal identifiable information ("PII") of Plaintiff and the other class members. Plaintiff asserts that this cyberattack occurred because Defendant failed to properly secure their network. Now before the Court is Defendant Teijin's Motion to Dismiss Plaintiff's Amended Complaint Pursuant to

Fed R. Civ. P 12(b)(6) (ECF No. 12). The Court finds that the briefing adequately addresses the issues in contention and dispenses with a hearing pursuant to E.D. Mich. L. R. 7.1(f)(2).

I. FACTUAL AND PROCEDURAL BACKGROUND

A. Plaintiff's Original Complaint (ECF No. 1) and Defendant's First Motion to Dismiss (ECF No. 8).

On February 8, 2023, Plaintiff, through her counsel, filed a complaint against Defendant initiating this matter. (ECF No. 1). Plaintiff brought this suit on behalf of herself and a class of similarly situated individuals, current and former employees of Defendant, whose personal identifiable information was compromised during the cyberattack. Plaintiff alleges, that Defendant is responsible for the injuries she suffered after her data was leaked since Defendant failed to properly safeguard it despite repeated warnings that ransomware attacks such as these were increasing. (ECF No. 10, PageID.110). On April 17, 2023, Defendant filed a Motion to Dismiss Plaintiff's Complaint in its entirety for failure to state a claim Pursuant to Fed. R. Civ. P. 12(b)(6). (ECF No. 8).

B. Plaintiff's Amended Complaint (ECF No. 10) and Defendant's Second Motion to Dismiss (ECF No. 10).

Plaintiff did not respond to Defendant's Motion to Dismiss. Instead, on May 8, 2023, Plaintiff filed an Amended Complaint, which included additional

allegations of the injuries she suffered as a result of the data breach. (ECF No. 10, PageID.122). *See* Fed. R. Civ. P. 15(a)(1)(B) (permitting a party to "amend its pleading once as a matter of course within … 21 days after service of a motion under Rule 12(b)"). The Court then denied Defendant's Motion to Dismiss as moot. *Crawford v. Tilley*, 15 F.4th 752, 759 (6th Cir. 2021) ("The general rule is that filing an amended complaint moots pending motions to dismiss.").

Plaintiff's Amended Complaint contains three counts, each of which stems from this single cyberattack. Count I states a negligence claim. (ECF No. 10, PageID.131). Count II states an implied breach of contract claim. (ECF No. 10, PageID.137). Count III seeks a declaratory judgment and injunctive relief. (ECF No. 10, PageID.139).

On May 5, 2023, Defendant filed a second Motion to Dismiss. (ECF No. 12). This motion seeks to dismiss Plaintiff's Amended Complaint in its entirety for failure to state a claim for relief pursuant to Fed. R. Civ. P. 12(b)(6). (ECF No. 12, PageID.150). On June 6, 2023, Plaintiff filed a Response to Defendant's Motion to Dismiss (ECF No. 13) and on June 26, 2023, Defendant filed a Reply in support of their Motion to Dismiss. (ECF No. 14). The facts giving rise to this case are set forth below.

C. Defendant was the victim of a cyberattack in December of 2020.

Defendant is a manufacturer of products used in the automotive, heavy, truck, marine, and recreational vehicles industries. (ECF No. 12, PageID.160). Throughout the course of its ordinary business, Defendant collects and stores its employees' PII including names, addresses, dates of birth, Social Security Numbers, health insurance information, and, in some cases, banking information. (ECF No. 10, PageID.98–99). Plaintiff is an employee of Teijin whose PII was collected and stored by the company. (ECF No. 12, PageID.160).

On December 1, 2022, Teijin became aware of a cyberattack in which cybercriminals held the company's digitally stored PII for ransom. (ECF No. 12, PageID.160). On December 13, 2022, Teijin notified its employees, including Plaintiff, about the data breach and urged them to take precautionary measures such as changing their personal passwords, remaining vigilant for any suspicious activity, and notifying financial institutions of fraud. (ECF No. 10, PageID.105).

On February 2, 2023, Defendant posted a press release on their website. (ECF No. 10, PageID.106). The press release explained that on November 30, 2022, a company employee clicked the link of a phishing email, which gave hackers access to the company's servers. (ECF No. 10, PageID.107). These servers contained information pertaining to current and former employees' participation in the company's health plan (*Id.*). The company CEO apologized for the data breach and assured that the company had since taken further steps to secure and safeguard

employee PII. (*Id.*). Neither the details of the breach, such as what specific IT vulnerabilities were exploited, nor the specific subsequent remedial measures implemented after the cyberattack, were ever disclosed to Plaintiff, the Class Members, or regulators. (ECF No. 10, PageID.109).

D. Prior to the breach, Defendant was or had reason to be on heightened notice of the potential for cyberattacks based on several warnings.

Plaintiff contends that Defendant knew or should have known that the company was at a heightened risk for cyberattack based on warnings that had been given by several organizations. (ECF No. 10, PageID.110). In October 2019, the Federal Bureau of Investigation published an article warning that hackers were targeting healthcare organizations, industrial companies, and the transportation sector for ransomware attacks. (*Id.*). In April 2020, ZDNet released an article stating that ransomware gangs were aggressively pursuing large companies to leak corporate information onto the dark web. (*Id.*). In September 2020, the United States Cybersecurity and Infrastructure Security Agency published an online ransomware guide advising that hackers have been extorting victims by threatening to release stolen data if victims did not pay their ransom demands. (ECF No. 10, PageID.111). Plaintiff believes that, based on these warnings, Defendant had reason to be on guard for cyberattacks and should have implemented security measures to protect employee PII. (ECF No. 10, PageID.112–117).

E. Plaintiff's information was "likely" compromised by the cyberattack and she suffered injuries as a result of the cyberattack.

At the time of the cyberattack, Plaintiff was employed by Defendant. (ECF No. 10, PageID.121). Therefore, Plaintiff's PII may have been accessed by hackers during the cyberattack. (ECF No. 10, PageID.122). This caused Plaintiff emotional distress and anxiety. (*Id*.). Further, on December 14, 2022, two days after the breach, an unknown and unauthorized individual fraudulently applied for and received a loan for $6,000.00 using Plaintiff's name and Social Security number. (*Id*.). Although the bank ultimately determined that the loan application was fraudulent and Plaintiff was not held responsible for it, Plaintiff incurred a $19.80 cost in order to send a police report and other information to the bank. (ECF No. 10, PageID.122). Additionally, as a result of the breach, Plaintiff spent time and resources self-monitoring her accounts in order to identify other fraudulent activity. (ECF No. 10, PageID.123). She also faces an increased risk of future fraud, identity theft, and misuse of her PII, all because of the data breach. (*Id*.).

II. LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(6) allows for the dismissal of a case where the complaint fails to state a claim upon which relief can be granted. When reviewing a motion to dismiss under Rule 12(b)(6), a court must "construe the complaint in the light most favorable to the plaintiff, accept its allegations as true, and draw all

reasonable inferences in favor of the plaintiff." *Handy-Clay v. City of Memphis*, 695 F.3d 531, 538 (6th Cir. 2012). To state a claim, a complaint must provide a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). "[T]he complaint 'does not need detailed factual allegations' but should identify 'more than labels and conclusions.'" *Casias v. Wal–Mart Stores, Inc.*, 695 F.3d 428, 435 (6th Cir. 2012) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007)).

The court "need not accept as true a legal conclusion couched as a factual allegation, or an unwarranted factual inference." *Handy-Clay*, 695 F.3d at 539 (internal citations and quotation marks omitted). In other words, a plaintiff must provide more than a "formulaic recitation of the elements of a cause of action" and his or her "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555–56. The Sixth Circuit has explained that, "[t]o survive a motion to dismiss, a litigant must allege enough facts to make it plausible that the defendant bears legal liability. The facts cannot make it merely possible that the defendant is liable; they must make it plausible." *Agema v. City of Allegan*, 826 F.3d 326, 331 (6th Cir. 2016) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

When ruling on a motion to dismiss, the Court may consider the complaint as well as (1) documents that are referenced in the plaintiff's complaint and that are

central to the plaintiff's claims, (2) matters of which a court may take judicial notice, (3) documents that are a matter of public record, and (4) letters that constitute decisions of a governmental agency. *Thomas v. Noder-Love*, 621 F. App'x 825, 829 (6th Cir. 2015); *Armengau v. Cline*, 7 F. App'x 336, 344 (6th Cir. 2001) ("We have taken a liberal view of what matters fall within the pleadings for purposes of Rule 12(b)(6).").

III. CHOICE OF LAW[1]

Under *Erie*, "federal courts sitting in diversity apply state substantive law and federal procedural law." *Gasperini v. Ctr. for Humans., Inc.*, 518 U.S. 415, 427 (1996) (citing *Erie R. Co. v. Tompkins*, 304 U.S. 64, 76 (1938). Choice-of-law rules are substantive, thus, a federal court sitting in diversity must apply the choice-of-law rules of the forum state. *Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496 (1941). Therefore, this Court applies Michigan's choice-of-law rules in determining which state's substantive law governs this action.

A. Michigan law applies to Plaintiff's negligence claim.

Under Michigan's choice-of-law rules for torts cases, courts "apply Michigan law unless a rational reason to do otherwise exists." *Sutherland v. Kennington Truck*

[1] Plaintiff does not address the issue of choice-of-law in their Amended Complaint. Defendant only analyzes choice-of-law regarding Plaintiff's negligence claim and finds that Michigan law applies. (ECF No. 12, PageID.164).

Serv., Ltd., 454 Mich. 274, 286 (1997) (internal quotations omitted). Courts apply a two-step analysis to determine whether any rational reason to depart from Michigan law exists. First, they "determine if any foreign state has an interest in having its law applied. If no state has such an interest, the presumption that Michigan law will apply cannot be overcome." *Id.* Next, if another state "does have an interest in having its law applied, [courts] determine if Michigan's interests mandate that Michigan law be applied" despite the other state's interest. *Id.*

Applying this framework, Michigan law governs this action. Here, Ohio has some interest in having their law applied since Plaintiff resides there. (ECF No. 10, PageID.103). This interest is, however, not strong enough to displace the presumption in favor of Michigan law considering the connection Michigan has to the case. Defendant's principal place of business is in Michigan and the leaked PII was collected and stored in Michigan. (ECF No. 10, PageID.104). Therefore, Michigan law governs this action.

B. Michigan law applies to plaintiff's breach of contract claim.

Michigan applies the most significant relationship test (Restatement (Second) of Conflict of Laws § 188) when resolving contract law conflicts. *Amerisure Mut. Ins. Co. v. Transatlantic Reinsurance Co.*, 573 F. Supp. 3d 1176, 1183 (E.D. Mich. 2021) (citing *Chrysler Corp. v. Skyline Indus. Servs., Inc.*, 448 Mich. 113, 124, (1995)). Under this test, the law of the state, which "has the most significant

relationship to the transaction and the parties" will apply. *Stone Surgical, LLC v. Stryker Corp.*, 858 F.3d 389 (6th Cir. 2017). To determine this, courts consider: "the place of contracting, the place of negotiation of the contract, the place of performance, the location of the subject matter of the contract, and the domicil, residence, nationality, place of incorporation and place of business of the parties." *Id*. at 389 (quoting Restatement (Second) of Conflict of Laws § 187) (internal quotations omitted). In the present dispute, these factors weigh in favor of Michigan law.

Plaintiff alleges that she and Defendant entered an implied contract whereby she agreed to submit her PII to Defendant as a condition of her employment and, in turn, Defendant agreed to "safeguard and protect" said PII. (ECF No. 10, PageID.137). The record offers no insight as to where the places of contracting or negotiation were, so those factors remain inconclusive. Plaintiff does, however, allege that Defendant "collect[ed] and/or stor[ed] the PII of Plaintiff" in Michigan. (ECF No. 10, PageID.104). Since, under Plaintiff's theory, Defendant's contractual obligations were to safeguard the PII, which was stored in Michigan, Defendants place of performance was Michigan. Similarly, the subject of the contract, the PII itself, was also located in Michigan. Finally, regarding the fifth factor, Michigan once again has the most significant relationship. While Defendant is incorporated in Delaware, it maintains its principal place of business in Michigan. (ECF No. 10,

PageID.104). And, while Plaintiff is a citizen of Ohio, she was employed in Michigan and a "substantial part of the events or omissions giving rise" to her claims occurred in Michigan. (ECF No. 10, PageID.104).

In sum, Michigan has the most significant relationship to this case based on the above five factors and, therefore, under Michigan's choice-of-law rules, Michigan law governs this claim.

C. Plaintiff's declaratory judgment claim is not a freestanding claim, rather it is a prayer for relief, so no independent choice-of-law analysis is required.

Count III of Plaintiff's complaint is a freestanding claim seeking declaratory judgment against Defendant. (ECF No. 10, PageID.139). As discussed below, declaratory judgment is a type of relief, rather than a freestanding claim, therefore, no independent choice-of-law analysis is required for this claim.

IV. DISCUSSION

A. Defendant's Motion to Dismiss Plaintiff's negligence claim should be denied because Plaintiff has pled Defendant's breach with the specificity needed to support a claim for relief.

Defendant's Motion to Dismiss Plaintiff's negligence claim argues that Plaintiff's allegations of the breach element are insufficient under *Iqbal* (556 U.S. at 681) and should be dismissed. To sustain a negligence claim, Plaintiff must establish that "(1) the defendant owed the plaintiff a legal duty, (2) the defendant breached the legal duty, (3) the plaintiff suffered damages, and (4) the defendant's breach was

a proximate cause of the plaintiff's damages." *Hill v. Sears, Roebuck & Co.*, 492 Mich. 651, 660 (2012). Defendant argues that Plaintiff failed to plead "the specific steps that the defendant could have or should have taken to prevent" the security breach from occurring and, therefore, has not pled the breach element of negligence. (ECF No. 12, PageID.164–165).

The thrust of Plaintiff's allegations of breach is that "Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach." (ECF No. 10, Page ID.134). Plaintiff lists these standards, rules, and regulations in detail. Plaintiff cites guidelines and recommendations promulgated by the United States Government, the United States Cybersecurity & Infrastructure Security Agency, and the Microsoft Threat Protection Intelligence Team on how organizations can safeguard against cyberattacks. (ECF No. 10, PageID.113–116). These recommendations include generic advice such as: "[i]mplement an awareness training program," "[s]et anti-virus and anti-malware programs to conduct regular scans," "[o]pen email attachments with caution," and "[t]horoughly investigate and remediate alerts" among many others (*Id.*).

Plaintiff does not, however, note which of these specific guidelines or recommendations Defendant failed to implement. Rather, Plaintiff relies on the occurrence of the data breach itself as "indicat[ion] that Defendant failed to

adequately implement one or more of the above measures to prevent ransomware attacks." (ECF No. 10, PageID.117). This logic is troubling because, as Defendant aptly notes, it requires "the Court to *infer* the breach of duty from the mere existence of the Cyberattack." (ECF No. 12, PageID.167). Were the court to make this inference, and find breach whenever a cyberattack succeeded, this would, in effect, create strict liability in data breach cases.

While the Sixth Circuit has yet to weigh in on this issue, other courts have dismissed similar broad and non-specific breach allegations as insufficiently pled under *Iqbal*. For example, in *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361 (S.D. Cal. Nov. 15, 2018), the plaintiff brought a statutory claim under California law after his PII was leaked during a cyberattack. The court dismissed this claim because of the plaintiff's failures to plead, with specificity, how the defendant's data storage and protection practices fell below the industry standard. In language equally applicable to our present case, the court asked: "What facts lead [the plaintiff] to believe [the defendant] didn't comply with industry standards? What are other companies doing that [the defendant] isn't? *Id.* at *2.

Plaintiff has failed to answer these same questions. Plaintiff's complaint lists ample industry standards (ECF No. 10, PageID.113–116), but fails to state, which specific standards Defendant failed to properly adopt. And, as the *Razuki* court notes:

> These are basic questions that [the plaintiff] could plead to plausibly show [the defendant's] conduct was unlawful. Instead, it appears [the plaintiff]

> simply recited a few buzz words with the hope that he may be able to figure out later what, if anything, [the defendant] has done wrong. But the Supreme Court tells us that's not enough.

Id. at *2. Other district courts have been equally demanding towards plaintiffs in their pleadings. In *Anderson v. Kimpton Hotel & Rest. Grp., LLC*, 2019 WL 3753308, *1 (N.D. Cal. Aug. 8, 2019), for example, the court held that the plaintiff's conclusory assertions that their "PII was left inadequately protected by [the defendant]" were not sufficient to sustain their claim. *See also Maag v. U.S. Bank, Nat'l Ass'n*, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021) (unsupported allegations that the defendant "failed to effectively monitor its systems for security vulnerabilities" were insufficient to support a claim); *Springmeyer v. Marriott Int'l, Inc.*, 2021 WL 809894, at *3 (D. Md. Mar. 3, 2021) ("mere repetition of conclusory and nonspecific allegations of [the defendant's] alleged shortcomings does not overcome the need to plead sufficient facts relating to what it did or did not do that led to the injuries").

Other courts have, however, been less demanding of plaintiffs at the pleading stage in data breach cases. In *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213 (11th Cir. 2023), for example, the Eleventh Circuit, reviewed the lower court's dismissal of the plaintiff's negligence action against his employer after a cyberattack compromised his PII. *Id*. at 1216. The district court found that the plaintiff had not sufficiently alleged the foreseeability of a cyberattack, which was required to

establish that the defendant owed him a duty, and dismissed the claim. *Id*. at 1220. On appeal, the Eleventh Circuit reversed this decision and noted that:

> [D]ata breach cases present unique challenges for plaintiffs at the pleading stage. A plaintiff may know only what the company has disclosed in its notice of a data breach. Even if some plaintiffs can find more information about a specific data breach, there are good reasons for a company to keep the details of its security procedures and vulnerabilities private from the public and other cybercriminal groups. We cannot expect a [party] in [plaintiff's] position to plead with exacting detail every aspect of [the defendant's] security history and procedures that might make a data breach foreseeable.

Id. In *Ramirez*, the Eleventh Circuit was discussing the duty element of negligence while the present case turns on the pleading requirements for the breach element. Nonetheless, the rationale applies equally here. In data breach cases, plaintiffs are at the mercy of their employers when it comes to collecting information about the specific procedures that were used to store their PII. Generally, they will know only what their employers choose to share, and employers have reason not to publicize their precise security procedures lest that information be used in further cyberattacks. This means that plaintiffs will often struggle to list specific data-security deficiencies until they can seek discovery from defendants.

This asymmetry of information was enough for the Eleventh Circuit and other lower courts to provide data breach plaintiffs with leeway at the pleading stage. *See In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 586 (N.D. Ill. 2022) (holding that the defendant adequately pled breach of duty by merely alleging

that the defendant "failed to implement one or more of the above measures" recommended by the United States Government "to prevent ransomware attacks."); *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *9 (S.D.N.Y. Mar. 23, 2021) (finding the plaintiff's complaint sufficient after alleging that the defendant failed "to implement certain safeguards and computer security practices that would have prevented disclosure of [PII].").

Textually, however, the *Iqbal* standard appears less generous. It states that: "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face."" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). Nothing in *Iqbal* indicates that this standard should be relaxed in data breach cases, nor in any of the multitude of cases where there is an asymmetry of information between plaintiff and defendant. Consider the facts of *Iqbal* itself for example. Javid Iqbal sued several federal officials including former Attorney General of the United States, John Ashcroft, as well as then Director of the Federal Bureau of investigation, Robert Mueller, on claims relating to the conditions of his detainment after he was arrested on criminal charges in the wake of the September 11, 2001, terror attacks. *Id*. at 666.

The defendants moved to dismiss Iqbal's complaint for failure to state a claim. *Id*. Ultimately, the case turned on whether Iqbal could plead, with the requisite factual particularity, that Ashcroft and Mueller, implemented the policies that led to

Iqbal's arrest, detention, and alleged mistreatment "for the purpose of discriminating on account of race, religion, or national origin." *Id*. at 676. If ever there was an asymmetry of information, it was in *Iqbal*. To defeat this motion, Javid Iqbal, a Pakistani Muslim living in post-September 11th America would have to plead, without the aid of any discovery, facts indicating that two of the most senior federal officials in the United States instituted a detention policy with the express intent of discriminating against him based on his religion, race, or national origin. Nonetheless, the Court applied the exacting *Twombly* standard and dismissed his case. *Id.* at 687.

For this reason, if all Plaintiff offered this Court were industry standards and conclusory statements, this Court might not be persuaded by the Eleventh Circuit's approach in *Ramirez*. Plaintiff, however, offers additional factual allegations, which are sufficient to defeat a motion to dismiss.

In addition to recitations of the various data-security guidelines and conclusory allegations that Defendant's practices fell below industry standards (ECF No. 10, PageID.113–117), Plaintiff's Complaint also specifically alleges that Defendant "could have prevented this Data Breach by properly securing and encrypting the folder, files, and or date fields containing [Plaintiff's] PII." (*Id*. PagedID.117). The Complaint further contends that Defendant's failure to use "basic

encryption techniques" constituted "conduct [which] created a foreseeable risk of harm to Plaintiff." (ECF No.10, PageID.133).

In response, Defendant argues that these allegations of failure to encrypt are no different than Plaintiff's other "conclusory allegations" and that the cases cited by Plaintiff do not "purport to recognize the alleged failure to encrypt data as *ipso facto* evidence of breach." (ECF No. 14, Page 200). Defendant is mistaken on both points.

First, unlike Plaintiff's other conclusory assertions that, because a data breach occurred, Defendant must have "failed to adequately implement one or more" of the industry standard safety measures (ECF No. 10, PageID.117), Plaintiff's contention that Defendant did not encrypt Plaintiff's PII is a specific factual allegation, which if true, could constitute breach of duty by Defendant. And, unlike the complaint's other conclusory statements, this factual allegation must be accepted as true when assessing the Motion to Dismiss. *Handy-Clay*, 695 F.3d at 539.

Defendant is equally mistaken in stating that courts have not found that a failure to encrypt PII can constitute a breach of duty. (ECF No. 14, Page 200). Plaintiff cites S*mallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175 (D. Nev. 2022). There, the court held that the plaintiff had met their pleading burden by alleging that the defendant retained the plaintiff's PII longer than necessary and "fail[ed] to encrypt the PII stores on its server" in addition to his general allegations that the

defendant deviated from industry best practices. *Id.* at 1189. These pleadings mirror Plaintiff's Complaint. Further, Defendant has failed to cite a single case, in which a court has held that an allegation that a party did not encrypt PII was insufficient evidence to plead breach of duty at the motion to dismiss stage.

For this reason, and because Plaintiff's complaint comports with the *Iqbal* standard outlined above, the Court denies Defendant's Motion to Dismiss Plaintiff's negligence claim for failure to state a claim.

It is worth noting, briefly, that Plaintiff's complaint alleges that Defendant also breached their duty of care by failing to "adequately and timely disclose to Plaintiff … the existence and the scope of the Data Breach." (ECF No. 10, PageID.135). However, as Defendant notes, Plaintiff "cites no factual basis for [this] bare conclusion" (ECF No. 12, PageID.166), and there are no facts in the record that indicate that Defendant's notifications of the breach were untimely or otherwise improper. The data breach occurred on December 1, 2022, and formal notice of breach was provided to Plaintiff on December 13, 2022. (ECF No. 12, PageID.160). Under the circumstances, and in the absence of any contrary allegations, there is no reason to assume the less than two-week delay in notification constitutes a breach of duty. Nonetheless, since Plaintiff's allegations that Defendant failed to encrypt her PII is itself sufficient evidence of breach, the failure of this argument is not fatal to Plaintiff's claim.

B. Defendant's Motion to Dismiss Plaintiff's claim for breach of implied contract should be denied because Plaintiff has pled all the required elements of the claim.

Under Michigan law, to sustain a claim for breach of contract, plaintiffs must plead: "(1) a contract, (2) [d]efendant's breach of the contract, and (3) damages to [p]laintiffs caused by the breach." *Emergency Dep't Physicians P.C. v. United Healthcare, Inc.*, 507 F. Supp. 3d 814, 827–828 (E.D. Mich. 2020) (citing *Bank of Am., NA v. First Am. Title Ins.*, 499 Mich. 74, 100–01 (2016). When no explicit contract exists between the parties "an implied contract may arise from their conduct, language, or other circumstances evidencing their intent to contract." *Lochridge v. Quality Temp. Servs., Inc.*, 2023 WL 4303577, at *7 (E.D. Mich. June 30, 2023) (citing *Featherston v. Steinhoff*, 226 Mich. App. 584 (1997)). An implied contract must still "satisfy the elements of mutual assent and consideration." *Mallory v. City of Detroit*, 181 Mich. App. 121, 127 (1989).

Plaintiff alleges that, as a requirement of her employment for Defendant, she was required to provide Defendant with her PII. (ECF No. 10, PageID.137). She further alleges that, in doing so, the parties entered an implied contract whereby "Defendant agreed to safeguard and protect [the] PII." (ECF No. 10, PageID.137).

Defendant contends that no implied contract was formed between the parties because there was neither mutual assent nor consideration regarding Defendant storing Plaintiff's PII. (ECF No. 12, PageID.168). Defendant further contends that,

even if a contract was formed, Plaintiff's claim for breach of contract still fails because she has not alleged that the breach was the proximate cause of any of plaintiff's damages. (ECF No. 12, PageID.171).

i. Plaintiff has pled that both parties gave consideration sufficient to create an implied contract.

To properly plead consideration, a party must show a bargained for exchange of legal value or detriment. *Emergency Dep't Physicians P.C.*, 507 F. Supp. 3d at 828 (citing *Higgins v. Monroe Evening News*, 404 Mich. 1, 20 (1978)). Under the preexisting legal duty rule, consideration is lacking when a party promises to perform an action for which they already have a preexisting legal duty to perform. *Id*. (citing *Yerkovich v. AAA*, 461 Mich. 732, 741 (2000)). Defendant argues that Plaintiff failed to plead consideration because neither she nor Defendant gave bargained-for-exchange for any implied agreement to safeguard the PII. (ECF No. 12, PageID.168–169).

First, Defendant claims that Plaintiff's Complaint fails to allege that "her provision of information to [Defendant] was part of an implicit agreement for [Defendant] to protect her PII from cyberattacks" and is thus insufficient consideration. (ECF No. 12, PageID.169). The Complaint, however, makes this allegation almost verbatim:

> Plaintiff and the Employee Subclass provided and entrusted their PII [to Defendant]. In doing so, Plaintiff and the Employee Subclass

> entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII.

(ECF No. 10, PageID.137). Defendant also fails to cite a single authority, which dismissed a similar claim of implied breach of contract for failure to plead consideration. In contrast, several cases have upheld implied breach of contract claims on similar facts. *See McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019) (finding the plaintiff met his burden by alleging that their employer implicitly agreed to safeguard their PII by requiring them to provide said information as a condition of employment); *Bowen v. Paxton Media Grp., LLC* 2022 WL 4110319, at *7 (W.D. Ky. Sept. 8, 2022) (finding *McKenzie* persuasive and holding the same).

Next, Defendant contends that the Complaint does not allege that Defendant gave any consideration in an implied contract to safeguard Plaintiff's PII under the preexisting legal duty rule. (ECF No. 12, PageID.169). Under the preexisting duty rule, "doing what one is legally bound to do is not consideration for a new promise." *Yerkovich*, 461 Mich. at 741 (citing *Puett v. Walker,* 332 Mich. 117, 122, 50 N.W.2d 740 (1952). "This rule applies whether the preexisting duty is based on statute or contract and whether the promise at issue is a modification to an existing agreement or whether it is a new agreement." *Romero v. Buhimschi*, 396 F. App'x 224, 233 (6th Cir. 2010) (citing *Kassab v. Dennis,* 2009 WL 763433 at *1 (Mich.Ct.App. Mar. 24, 2009)).

Earlier in her complaint, when discussing her negligence claim, Plaintiff asserts that Defendant owed her a duty to: "exercise reasonable care in safeguarding" her PII; "to exercise appropriate clearinghouse practices;" "to have procedures to detect and prevent [] improper access and misuses of PII" and, among other things, "to use reasonable security measures." (ECF No. 10, PageID.131–132). Defendant cites these portions of the Complaint and argues that, because Plaintiff has already alleged that Defendant owed her this duty of care rooted in negligence, under the preexisting legal duty rule, any implicit agreement to safeguard Plaintiff's PII was not sufficient consideration to create an implied contract. (ECF No. 12, PageID.169) Under Michigan law, however, the preexisting legal duty rule applies only to duties imposed by statute or contract. *Romero*, 396 F. App'x at 233 (6th Cir. 2010). Defendant cites no authority that suggests Michigan law applies the preexisting legal duty rule to duties arising under tort, nor is there reason to extend the rule in this way. If a duty imposed by tort created a preexisting legal duty, then plaintiffs would nearly always be precluded from suing defendants in both tort and contract for incidents arising out of the same operative facts. Plaintiff has, therefore, pled consideration sufficient to support the formation of an implied contract.

ii. Plaintiff has pled that the parties mutually assented to the implied contract.

An implied contract arises when parties show a mutual intent to contract with each other. *Kingsley Assoc., Inc., v. Moll PlastiCrafters, Inc.*, 65 F.3d 498, 504 (6th

Cir. 1995). This assent to contract can be deduced "from the conduct of the parties, language used, or things done by them, or other pertinent circumstances." *Erickson v. Goodell Oil Co., Inc.*, 384 Mich. 207, 212 (1970).

Defendant argues that Plaintiff has failed to plead mutual assent because her complaint does not allege "the terms of the purported contract, much less the conduct, language or other pertinent circumstances from which an agreement to be bound can be inferred" (ECF No. 12, PageID.170). In essence, Defendant believes that, since Plaintiff never alleged the parties "discussed, understood, or were aware of the necessary terms" of the contract, terms such as the specific measures Defendant would take to safeguard the PII or even the scope of the protection Defendant would provide, Plaintiff has failed to plead that there was a meeting of the minds. (ECF No. 12, PageID.170–171).

Nonetheless, courts around the country have found the existence of mutual assent even in the absence of clear definitive terms outlining the specific measures a party would take to protect PII. *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242 (N.D. Cal. Sept. 14, 2016) is illustrative. There, the court found that the plaintiff had sufficiently pled the existence of an implied contract by alleging simply that the plaintiff "would take adequate measures and make reasonable efforts to properly safeguard its employees[']' personal identifying information." *Id.* at *9 (cleaned up). In doing so, the court noted that:

> [T]o require a specifically pleaded scope of data protection for an *implied* breach of contract claim would operate to preclude such a claim between all but the most sophisticated and familiar parties. Even if the party sharing his or her data had very specific expectations about the measures that would be taken to protect it, it would be exceedingly difficult to show the recipient assented to those precise protective measures.

Id. Instead, the court found that plaintiff's general allegations of the existence of an implied contract presented a more realistic reflection of data-collecting agreements: "When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected." *Id*; *see also Savidge v. Pharm-Save, Inc.*, 2017 WL 5986972, at *9 (W.D. Ky. Dec. 1, 2017) (finding *Castillo* persuasive and holding that the plaintiffs had pled mutual assent by alleging that the defendants "implicitly promised … that they would take adequate measures to protect their sensitive and personal information."); *Foster v. Health Recovery Servs., Inc.*, 493 F. Supp. 3d 622, 640–41 (S.D. Ohio 2020) (finding that the plaintiff sufficiently pled an implied contract by alleging that the defendant "represented that it would keep [his PII] secure"); *Bowen*, 2022 WL 4110319, at *7 (the plaintiff met his pleading burden by alleging that the defendant agreed to "safeguard and protect" his PII).

Other courts have, however, rejected the idea that an implied promise to protect PII constitutes mutual assent. For instance, in *Ramirez*, the Eleventh Circuit held that the district court properly dismissed the plaintiff's breach of implied contract claim because the complaint failed to "allege any facts from, which we

could infer that [the defendant] agreed to be bound by any data retention or protection policy." *Ramirez*, 69 F.4th at 1221; *see also Antman v. Uber Techs., Inc.*, 2018 WL 2151231, at *12 (N.D. Cal. May 10, 2018) (dismissing the plaintiffs' claim because they pled "no facts about the existence of an implied contract" for the defendant to protect their PII).

Defendant would have this Court be persuaded by the Eleventh Circuit here[2] and dismiss Plaintiff's breach of implied contract claim. (ECF No. 14, PageID.202). Defendant believes that Plaintiff merely "points the Court to a handful of foreign cases finding data-protection agreements are implicit in an employment relationship." (ECF No. 14, PageID.201). Defendant notes that "[n]one of those cases is binding, analyzed whether mutual assent was pled, or even applied Michigan law." (*Id.*, PageID.201–2).

Only a few days after briefing was submitted in this case, a district court in this district decided a case, which both analyzed mutual assent and applied Michigan law. In *Lochridge v. Quality Temp. Servs., Inc.*, 2023 WL 4303577 (E.D. Mich. June 30, 2023) (Behm, J.)[3], the plaintiff brought a claim for breach of implied contract

[2] "here", because Defendant asks this Court to follow *Ramirez* in dismissing the implied breach of contract claim, but not to follow *Ramirez* in allowing Plaintiff's negligence claim to survive as discussed above.

[3] The Court recognizes that the parties did not have a chance to brief *Lochridge*, but notes that the Court's holding is based on the totality of the reasons discussed in this opinion and is not reliant on any single case.

against the defendant, a staffing agency, after their PII was compromised following a cyberattack. *Id*. at *1. The plaintiff alleged that the defendant required the plaintiff "to provide his information to utilize their services, thereby creating an implied contract that they would" protect the plaintiff's PII. *Id*. at *7. The court, applying Michigan law, held that this allegation was sufficient to plead the existence of an implied contract, and that, by arguing that the defendant "did not protect their information or notify them in a timely matter," the plaintiff stated a claim for breach of implied contract. *Id.*

Plaintiff's allegations in our present case are essentially identical to those that the Eastern District of Michigan and several other "courts in this circuit have found … sufficient to show a meeting of the minds" (*Id*.), and the logic behind these decisions is persuasive. Put succinctly, 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." *Castillo*, 2016 WL 9280242, at *9. As such, Plaintiff's allegations, sparse though they may be, allege mutual assent sufficient to state a claim for implied breach of contract.

iii. Plaintiff has pled that she suffered damages as a result of Defendant's breach of their implied contract.

Defendant next moves to dismiss Plaintiff's contract claim for failure to allege damages. (ECF No. 12, PageID.171). Under Michigan law, to properly state a claim for breach of contract, a plaintiff must plead that they suffered damages caused by

the breach. *Emergency Dep't Physicians P.C.*, 507 F. Supp. 3d at 828 (E.D. Mich. 2020) (citing *Bank of Am., NA*, 499 Mich. at 100–01). The party asserting breach "has the burden of proving its damages with reasonable certainty, and may recover only those damages that are the direct, natural, and proximate result of the breach." *Alan Custom Homes, Inc. v. Krol*, 256 Mich. App. 505, 512 (2003). Defendant contends that Plaintiff has failed to allege any "non-speculative contract damages that were *proximately* caused by the purported breach." (ECF No. 12, PageID.171)

Plaintiff's complaint, however, recites a host of alleged damages they suffered:

> As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Employee Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

(ECF No. 10, PageID.138–139). Courts have found similar allegations sufficient to plead proximate cause. *See McKenzie*, 369 F. Supp. 3d at 818 (finding that the plaintiff's essentially identical allegations of injury sufficiently pled proximate cause over the defendant's similar argument that they were too speculative).

Furthermore, even if, for arguments sake, these allegations are overly speculative, Plaintiff also specifically alleges that, two days after the data breach occurred, "an unknown and unauthorized individual applied for and obtained a $6,000.00 loan with FinWise Bank using Plaintiff's name and other information, including her Social Security number." (ECF No. 10, PageID.122). Although the bank ultimately caught the fraud, Plaintiff incurred a cost of $19.80 in postage while reporting the incident to the bank. (ECF No. 10, PageID.122). This amount, small though it may be, is a non-speculative damage that occurred as a proximate cause of the data-breach.

Defendant, however, maintains that even this allegation is insufficient, because Plaintiff does not specifically allege "that her personal information was actually on the dark web, or that the Cyberattack was the source of the information that was used to apply for the loan." (ECF No. 14, PageID.203). Despite these omissions, Plaintiff's allegations are sufficient.

In deciding whether a plaintiff has submitted a plausible claim, courts may "draw on [their] experience and common sense." *Iqbal*, 556 U.S. at 664. Plaintiff alleges that a cyberattack compromised the PII of employes at Teijin, and that, two days after this incident, a fraudulent loan was taken out in Plaintiff's name using her confidential information. (ECF No. 10, PageID.122). Given this timing, common sense would dictate that Plaintiff's information was indeed leaked during the

cyberattack. At very least, the timing makes this conclusion plausible enough to sustain a claim at this stage. Other courts have found similarly. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1318 (N.D. Ga. 2019) (allegations that the plaintiffs suffered some form of identity theft or other fraudulent activity following a cyberattack was "sufficient at the pleading stage to establish that the Data Breach was the proximate cause" of the plaintiffs' injuries).

The Sixth Circuit has, in the standing context, also found similar allegations sufficient to show causation and injury. In *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 385 (6th Cir. 2016) the plaintiffs brought suit against Nationwide Mutual Insurance Company after hackers breached the defendant's network and stole the plaintiffs' PII. The district court dismissed the plaintiffs' negligence claim for lack of Article III standing. *Id*. The Sixth Circuit reversed and held that the plaintiffs had sufficiently alleged that their injuries were fairly traceable to the defendants conduct by pleading that the defendant failed to properly secure their PII against anticipated threats of cyberattacks. *Id*. at 390. Although, the Sixth Circuit made clear that "causation to support standing is not synonymous with causation sufficient to support a claim," the holding in *Galaria* is nonetheless illustrative. *Id*. (quoting *Parsons v. U.S. Dep't of Just.*, 801 F.3d 701, 715 (6th Cir. 2015)). The Article III traceability requirement "eliminate[s] those cases in which a third party and not a party before the court causes the injury." *Id*. (quoting *Am. Canoe Ass'n v.*

City of Louisa Water & Sewer Comm'n, 389 F.3d 536, 542 (6th Cir. 2004). Therefore, if allegations like Plaintiff's here satisfy Article III traceability, then Defendant, not a third party, must have caused Plaintiff's injuries. While not dispositive, this goes a long way towards Plaintiff showing that her injuries were proximately caused by Defendant.

Finally, Defendant maintains that Plaintiff's claim fails because she cites no authorities applying Michigan law, in which a court upheld similar allegations of injuries as sufficient. (ECF No. 14, PageID.203). In *Lochridge*, however, a court in this district, applying Michigan law, did just that. There, the defendant sought to dismiss the plaintiff's negligence claim for failure to allege injury. *Lochridge*, 2023 WL 4303577 at *6. The Court noted that, while:

> [d]amages 'incurred in anticipation of possible future injury rather than in response to present injuries,' are not cognizable under Michigan law the fact that Plaintiff alleges that his information was already used to fraudulently open an account and apply for a loan is sufficiently concrete to state a claim.

Id. (internal citations omitted). Plaintiff's allegation in our present case, that an unauthorized loan was taken out in her name following the cyberattack (ECF No. 10, PageID.122), is the same allegation set forth by the *Lochridge* plaintiff. If that was sufficient to state a plausible claim of injury under Michigan law, Plaintiff's claim here must be sufficient as well. While the *Lochridge* court was discussing these allegations in the context of a negligence claim, and we look at them as they

relate to Plaintiff's breach of contract claim, this distinction is immaterial. Both causes of action require the plaintiff to show damages proximately caused by the defendant, so the analysis remains the same.

For these reasons Plaintiff has pled that she suffered an injury proximately caused by Defendant sufficient to state a plausible claim of implied breach of contract.

C. Defendant's Motion to Dismiss Plaintiff's claim for declaratory and injunctive relief should be granted because Plaintiff lacks standing for these remedies.

Count III of Plaintiff's complaint seeks a declaratory judgment and injunctive relief. (ECF No. 10, PageID.139). Plaintiff requests that this Court declare that Defendant has a duty to secure Plaintiff's PII, that they continue to breach this duty by not using reasonable security measures, and that the ongoing breach continues to cause Plaintiff harm. (ECF No. 10, PageID.140). Plaintiff also seeks injunctive relief requiring Defendant to employ additional security measures to better safeguard the PII. (ECF No. 10, PageID.141). Defendant seeks to dismiss this claim as well, arguing that these are remedies, rather than standalone causes of action. (ECF No. 12 PageID.172).

Under the Declaratory Judgment Act, a court may issue declaratory judgment in "case[s] of actual controversy." 28 U.S.C. § 2201(a). The Declaratory Judgment Act does not provide an independent standalone cause of action, it is merely a

remedy. *Davis v. United States*, 499 F.3d 590, 594 (6th Cir. 2007) (citing *Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950)). In considering whether to grant declaratory relief courts should consider:

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

Larry E. Parrish P.C. v. Bennett, 989 F.3d 452, 457 (6th Cir. 2021) (citing *Grand Trunk W. Rail Co. v. Consolidated Rail Corp.*, 746 F.2d 323, 326 (6th Cir. 1984)). Before considering these five factors, a court must first establish whether the basic jurisdictional requirements have been met, such as whether the plaintiff has demonstrated standing for each claim and for each form of relief sought. *Lochridge*, 2023 WL 4303577 at *8. When, as is the case here, the alleged injury is a future injury "the plaintiff must demonstrate that the threatened injury is certainly impending or there is a substantial risk that the harm will occur." *Id*. (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)).

Plaintiff has failed to do so here. Plaintiff has stated plausible claims for injuries that have already occurred because of this data-breach and for injuries that might occur in the future as a result of this data-breach. Plaintiff's request for declaratory judgment and injunctive relief, however, would not redress these

injuries, rather, they seek to prevent a second breach from occurring. In *Lochridge*, the court found similarly, that the plaintiff, who sought essentially the same declaratory judgment and injunctive relief, had not met the jurisdictional requirements for this relief because he had not "alleged any facts tending to show that a second data breach is currently impending or there is a substantial risk that one will occur." *Id*. The same is true here.

By failing to allege any facts, which would suggest Defendant is at risk for a second cyberattack, Plaintiff has failed to meet the jurisdictional requirements of this relief. *See also Hall v. Centerspace, LP*, 2023 WL 3435100, at *4 (D. Minn. May 12, 2023) (holding that the plaintiff had no standing for similar injunctive relief because his complaint failed to "indicate a second data breach is certainly impending, or even that there is a substantial risk one will occur."). Therefore, Plaintiff's claims for declaratory and injunctive relief should be dismissed.

V. CONCLUSION

For the above reasons, the Court, taking the facts in the light most favorable to the non-moving party, grants Defendant's Motion to Dismiss Plaintiff's Amended Complaint (ECF No. 12) in part, and denies it in part. The Court:

(1) **DENIES** Defendant's Motion to Dismiss as to Plaintiff's negligence claim (Count I);

(2) **DENIES** Defendant's Motion to Dismiss as to Plaintiff's breach of implied contract claim (Count II);

(3) **GRANTS** Defendant's Motion to Dismiss as to Plaintiff's declaratory judgment claim (Count III).

IT IS SO ORDERED.

Dated: September 20, 2023

s/Paul D. Borman
Paul D. Borman
United States District Judge