UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

RODNEY JOHNSON, individually and on behalf of all others similarly situated,
Plaintiff,

v. **Case No. 25-cv-687**

90 DEGREE BENEFITS, INC.,
Defendant.

DECISION AND ORDER

Plaintiff Rodney Johnson commenced this class action against defendant 90 Degree Benefits, Inc. on May 12, 2025. Plaintiff alleges that defendant failed to secure the personal information of its customers, leading to that information being stolen in a hacking incident. Defendant filed a motion to dismiss plaintiff's first amended complaint on August 14, 2025, for lack of subject-matter jurisdiction and for failure to state a claim. Fed. R. Civ. P. 12(b)(1), (6). For the reasons that follow, defendant's motion is granted in part and denied in part. Plaintiff is granted leave to amend.

I. BACKGROUND

As plaintiff alleges, defendant is a company that designs health plans and administers healthcare benefits. (Am. Compl. ¶ 2.) A hacker gained access to defendant's computer network on or about October 18, 2024, and accessed the Personally Identifiable Information ("PII") and/or Personal Health Information ("PHI") of plaintiff and several thousand other individuals. (*Id.* ¶ 5.) Defendant notified the impacted individuals on or about March 10, 2025, that their information may have been accessed. (*Id.* ¶ 8.) Plaintiff now fears that his information may be sold to criminals and/or used to commit identity theft or other harms at some point in the future. (*Id.* ¶¶ 9, 11.)

II. JURISDICTION

Plaintiff argues that this court has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) because the complaint asserts a class action with an amount in controversy over $5,000,000. Plaintiff also asserts that he is a citizen of California, and that defendant is a citizen of Wisconsin, satisfying minimal diversity.

III. DISCUSSION

Defendant argues that this court lacks subject-matter jurisdiction because the amended complaint fails to establish Article III standing. Alternatively, defendant argues that the amended complaint fails to state a claim upon which relief may be granted.

A. Article III Standing

Federal courts have limited jurisdiction and must dismiss any action where subject-matter jurisdiction is lacking. *Kokkonen v. Guardian Life Ins. Co. of America*, 511 U.S. 375, 377 (1994); Fed. R. Civ. P. 12(h)(3). The subject-matter jurisdiction of federal courts is limited to deciding only "Cases" and "Controversies." U.S. Const. art. III, § 2. A plaintiff may assert a case or controversy only if he or she has standing—that is, "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). Standing is not dispensed in gross and must be shown for each form of relief sought. *Friends of the Earth, Inc. v. Laidlaw Environ. Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000). In short, a federal case must contain "a real controversy with real impact on real persons." *Am. Legion v. Am. Humanist Assoc.*, 588 U.S. 29, 87 (2019) (Gorsuch, J., concurring).

Plaintiff alleges that hackers obtained the PII/PHI of himself and other class members, which may include names, dates of birth, home addresses, phone numbers, Social Security numbers, driver's license numbers, medical information, and health insurance information, due to defendant's negligent cybersecurity practices. This breach puts the class members at

"significant risk of identity theft and various other forms of personal, social, and financial harm" for the rest of their lives. (Am. Compl. ¶ 11.) Specifically, plaintiff has suffered:

- inherent harm for the theft of his personal information and invasion of privacy;
- costs associated with detecting and preventing identity theft;
- time spent, and lost productivity associated with, mitigating the consequences of the data breach;
- emotional distress, anguish, stress, and annoyance;
- actual and/or imminent injury arising from actual and/or potential fraud and identity theft by ill-intentioned hackers and/or criminals;
- diminution in value of his personal information by its unlawful dissemination;
- continued risk to the data still held by Defendant so long as Defendant fails to adopt adequate measures to safeguard the PII and PHI in its custody.

(Am. Compl. ¶ 14.) Plaintiff claims to have spent "additional time reviewing his bank statements, credit cards, and reviewing his emails for fraud alerts." (*Id.* ¶ 22.) Going forward, plaintiff intends to continue mitigating harm by "continually reviewing his depository, credit, and other accounts for unauthorized activity." (*Id.* ¶ 23.)

Defendant asserts that the amended complaint fails to allege a concrete injury-in-fact. In defendant's view, plaintiff has not alleged that he suffered any actual or attempted identity theft or misuse of his data, nor does he allege any resulting out-of-pocket monetary loss. Rather, defendant argues that plaintiff's "injury" contains only speculative future harm, abstract emotional harm, and self-incurred costs, and none are sufficient under Article III.

A sufficient injury is one that is "concrete and particularized," as well as "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (cleaned up). Similar to the rule stated in *Twombly* and *Iqbal* that a plaintiff must allege facts showing a "plausible claim of relief," the same standard applies to standing. *Silha v. ACT, Inc.*, 807 F.3d 169, 173–74 (7th Cir. 2015) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544

(2007); *Ashcroft v. Iqbal*, 556 U.S. 662 (2009)). The plaintiff's well-pled factual allegations, stripped of their legal conclusions, must show that Article III standing is plausible on the face of the complaint. Additionally, the named plaintiff must have suffered the same injury as the class as a whole. *Payton v. Cnty. of Kane*, 308 F.3d 673, 682 (7th Cir. 2002) (citing *Allee v. Medrano*, 416 U.S. 802, 828–29 (1974) (Burger, C.J., dissenting)).

On the risk of harm itself, and on plaintiff's voluntary mitigation measures, both parties draw parallels to this case and the decision in *Dusterhoft v. OneTouchPoint Corp.*, No. 22-cv-882-bhl, 2024 WL 4263762 (E.D. Wis. Sept. 23, 2024). There, Judge Ludwig found that all named plaintiffs lacked standing to pursue money damages for the "mere risk of future identity theft." *Dusterhoft*, 2024 WL at *6 (citing *TransUnion v. Ramirez*, 594 U.S. 413, 441 (2021)). The court also found that allegations for "diminution in the value of plaintiffs' private information" were too conclusory under the *Iqbal* standard to find standing. *Id.* (citing *Silha*, 807 F.3d at 174). Applying these principles to this case, I likewise agree that plaintiff's claim for diminution in value of private information is not concrete enough to establish an injury-in-fact and is inadequately pled to boot. *See Giasson v. MRA – Management Assoc., Inc.*, 777 F.Supp.3d 913, 929–30 (E.D. Wis. Apr. 7, 2025) (Stadtmueller, J.) (collecting cases). I also conclude that *TransUnion* forecloses plaintiff's claim for the risk of future harm. *TransUnion*, 594 U.S. at 436 ("[T]he mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm.").

However, the *Dusterhoft* court found that some named plaintiffs did allege standing to seek damages for the harm of "time and money spent by plaintiffs" to mitigate the risk of future identity theft. *Id. Dusterhoft* explained that the Seventh Circuit's jurisprudence, even post-*TransUnion*, leaves open the potential for standing where the plaintiff undertook efforts to mitigate risk in the face of "an imminent or certainly impending risk of harm as a result of

the breach." *Id.* (citing *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692 (7th Cir. 2015)) (cleaned up). This was enough, it reasoned, in light of the complaint's lengthy allegations on the general risk of cyberattacks and data breaches, allegations that some plaintiffs suffered "actual identity theft and fraud as a result of the breach," and detailed allegations of specific mitigation efforts undertaken by certain named plaintiffs. *Id.* at *7. One named plaintiff (Dusterhoft), however, had not shown standing because he alleged only that he "*anticipates* spending considerable time and money . . . to mitigate and address harms caused by the Data Breach." *Id.* (emphasis added). The court found this to be an impermissible future injury.

As for injunctive and declaratory relief, the court found that allegations of future injury from a successive data breach were "too conjectural." *Id.* The plaintiffs had not plausibly alleged enough facts to suggest that the defendant was at "imminent risk" of a future data breach, just the vague allegation that its security practices remain inadequate. *Id.* And an injunction against the defendant would do nothing to prevent third-party criminals from misusing the information already leaked. *Id.* Likewise, a declaratory judgment would do nothing to redress the alleged harm. *Id.* at *8.

Notwithstanding the fact that *TransUnion* "marked a shift in the [Supreme] Court's standing jurisprudence," I agree with the court in *Dusterhoft* that we are still bound by some of the Seventh Circuit's decision in *Remijas*.[1] *Dinerstein v. Google, LLC*, 73 F.4th 502, 516 (7th Cir. 2023). There, the Seventh Circuit held that the increased risk of identity theft from a data breach was inherently a "certainly impending future harm" that qualified for Article III

[1] The Seventh Circuit suggested in passing that *Remijas* remains "authoritative," at least in part. *See Dinerstein v. Google, LLC*, 73 F.4th 502, 516 (7th Cir. 2023) ("Our decisions in [*Remijas*] and [*Lewert*] are not to the contrary. As an initial matter, both predate *TransUnion*. While that is not to say that they are no longer authoritative, it is to recognize that *TransUnion* marked a shift in the [Supreme] Court's standing jurisprudence.")

standing. *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 966 (7th Cir. 2016) (citing *Remijas*, 794 F.3d at 692) (internal quote omitted). It separately held that costs previously incurred to mitigate the risk of future identity theft could be sufficient injuries. *Remijas*, 794 F.3d at 694. While *TransUnion* did away with standing for claims alleging "mere risk of future harm" and seeking money damages, it held open the potential for standing where that risk of future harm caused a separate past harm. *TransUnion*, 594 U.S. at 436. This new rule still allows for standing where the plaintiff allegedly incurred reasonable costs to mitigate the effect of a data breach. *Lewert*, 819 F.3d at 967. The exact boundaries of "reasonable" efforts following a data breach are less clear, but many courts have found that lost time may constitute a concrete harm. *See id.* (finding that "time and effort" monitoring for identity theft is sufficient for standing).

Plaintiff alleges that he "spent additional time reviewing his bank statements, credit cards, and reviewing his emails for fraud alerts." (Am. Compl. ¶ 22.) Despite the caselaw seeming to support plaintiff's claim to standing, defendant tries to distinguish plaintiff's allegations from *Dusterhoft* for lack of detail. For instance, defendant notes that the *Dusterhoft* plaintiffs alleged they spent at least an hour on mitigation efforts, and in some cases multiple hours. In another example, the *Lewert* plaintiff allegedly spent exactly $106.89 for credit monitoring services. While plaintiff's harm allegations are admittedly vague and border on conclusory, defendant has not shown, for instance, that courts in this circuit apply a bright line between *de minimis* efforts and greater efforts. If that were the case, I might agree that a specific amount of time is needed to move the allegation beyond "possibility" to "plausibility." *Iqbal*, 556 U.S. at 678. But detail for the sake of detail is not needed at the pleading stage.

Defendant further points out that some of the *Dusterhoft* plaintiffs suffered actual identity theft, unlike plaintiff. Even though true, this distinction fares no better than the last. While such an allegation might have made the plaintiffs' mitigation efforts appear more

reasonable, or might make the risk of identity theft for other plaintiffs appear more "certainly impending," it is not a *per se* requirement to allege standing. *See Remijas*, 794 F.3d at 693 ("[Data breach victims] should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing. . ."). Therefore, I must conclude that plaintiff has pled standing as to his claim for damages.

However, I concur with the reasoning of *Dusterhoft* and find that the plaintiff lacks standing as to injunctive and declaratory relief. Plaintiff has failed to show that the harms he alleges would be redressed by either an injunction or declaration. To start, an injunction requiring that defendant adopt new security measures or delete plaintiff's data would not reduce the threat of identity theft using the PII/PHI already taken. More importantly, plaintiff has not pled sufficient facts to suggest that a future data breach is "certainly impending" absent an injunction. *Clapper*, 568 U.S. at 410. The fact that a data breach occurred in the past, and even that this is defendant's second recent data breach, does not inherently make another imminent data breach "plausible" as opposed to possible. *Iqbal*, 556 U.S. at 678. Beyond that, plaintiff's only other allegation supporting an injunction is that defendant's data practices remain insufficient. (Am. Compl. ¶ 155.) Like in *Dusterhoft*, this statement is conclusory because it fails to allege *how* or *why* defendant's practices remain inadequate.

Briefly addressing declaratory relief, I find that a declaratory judgment would not redress any of plaintiff's alleged injuries. Redressability is a separate essential element of Article III standing. *Lujan*, 504 U.S. at 560. The amended complaint fails to suggest what a declaration of plaintiff's rights would accomplish. At most, it states that Cal. Code Civ. § 1798.150(a)(1)(B) permits declaratory relief among other remedies. (*Id.* ¶ 126.) But plaintiff does not identify, nor can I, any remedial purpose it would serve in this case. Without showing that relief from his injury with a declaration is "likely, as opposed to merely speculative," plaintiff cannot proceed on that form of relief. *Lujan*, 504 U.S. at 560.

In summary, plaintiff has pled Article III standing as to his claim for money damages, but not for injunctive or declaratory relief.

B. Common Law Negligence

Defendant moves to dismiss plaintiff's claim for tortious negligence under Rule 12(b)(6) for failure to state a claim. To state a claim upon which relief may be granted, a complaint must "state a claim that is plausible on its face." *Twombly*, 550 U.S. at 570. "A claim has facial plausibility 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. The complaint must, at a minimum, "give the defendant fair notice of what the claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555. In evaluating a motion to dismiss under Rule 12(b)(6), I must "accept the well-pleaded facts in the complaint as true"; however, "legal conclusions and conclusory allegations merely reciting the elements of the claim are not entitled to this presumption of truth." *McCauley v. City of Chicago*, 671 F.3d 611, 616 (7th Cir. 2011).

Plaintiff has conceded by silence that substantive Wisconsin law applies to his claim for negligence, and defendant asserts that Wisconsin law applies. *See McCoy v. Iberdrola Renewables, Inc.*, 760 F.3d 674, 684 (7th Cir. 2014) ("When no party raises the choice of law issue, the federal court may simply apply the forum state's substantive law."). The traditional elements of negligence in Wisconsin are a duty of care, breach of that duty, injury, and a causal connection between the breach and injury. *Hoida, Inc. v. M & I Midstate Bank*, 2006 WI 69, ¶ 23, 717 N.W.2d 17 (2006).

Defendant argues that plaintiff has not alleged to have suffered an injury that satisfies Wisconsin tort law: "actual loss or damage resulting from the injury." *Gritzner v. Michael R.*, 2000 WI 68, ¶ 19, 611 N.W.2d 906 (2000). As relevant here, a tort claim is "not capable of present enforcement" until the plaintiff has suffered "harm that has already occurred or is

reasonably certain to occur in the future," "not the mere possibility of future harm." *Hennekens v. Hoerl*, 160 Wis.2d 144, 152–53, 465 N.W.2d 812 (Wis. 1991) (cleaned up). Plaintiff counters that, at the pleading stage, the standard for alleging an injury as an element of negligence is no greater than what is required to allege an injury-in-fact for standing.

Confounding my analysis is the tendency of Wisconsin state courts to resolve similar questions under state standing doctrine rather than as an element of the cause of action. *See, e.g., Baysal v. Am. Family Life Ins. Co.*, 2025 WI App 78, 28 N.W.3d 926 (2025); *Bauer v. Fincantieri Marine Group, LLC*, No. 2024AP1882, 2025 WL 3210945 (Wis. Ct. App. Nov. 18, 2025) (petition for review filed). One exception is *Reetz v. Advocate Aurora Health, Inc.*, where the Court of Appeals held that the data breach plaintiff had pled "actual damages" as an element of negligence after experiencing "fraudulent transactions and resulting overdraft fees in her bank account." 2022 WI App 59, ¶¶ 11–13, 983 N.W.2d 669. This opinion notes that fraudulent transactions, even after the bank reverses them as fraudulent, may give rise to an injury due to the "value of one's own time needed to set things straight[.]" *Id.*, ¶ 12 (quoting *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2022)). It also notes, with an unclear amount of weight given to the fact, that data breaches tend to increase the risk of identity theft. *Id.* (citing *Lewert*, 819 F.3d at 966). As defendant notes, however, the plaintiff in *Reetz* alleged actual identity theft following a data breach. It is a useful opinion, but that detail is critical.

Given that limitation, I find a more recent decision by the Wisconsin Court of Appeals to be instructive. The recent decision in *Bauer v. Fincantieri Marine Group* concerns a data breach *without* an allegation of actual identity theft and is analyzed under Wisconsin's own standing doctrine. No. 2024AP1882, 2025 WL 3210945 (Wis. Ct. App. Nov. 18, 2025) (petition for review filed). Here, the Wisconsin Court of Appeals held that "*Reetz* does not support a conclusion that a threat of future identity theft *alone* is sufficient to establish

standing in Wisconsin." *Id.*, ¶ 16 (emphasis in original). Moreover, "*Reetz* does not support the proposition that the entirely prospective and hypothetical risk of identity theft—or the expenditures undertaken to guard against that hypothetical risk—are sufficient to establish standing under Wisconsin law." *Id.*

In Wisconsin courts, a plaintiff has "standing" when they show (1) a personal interest in the controversy, (2) an injury, and (3) that vindicating their claim is consistent with judicial policy. *Foley-Ciccantelli v. Bishop's Grove Condo. Ass'n, Inc.*, 2011 WI 36, ¶ 40, 797 N.W.2d 789. While not bound by Article III's "Cases" or "Controversies" requirement, Wisconsin courts often look to federal standing doctrine as guiding. *Friends of Black River Forest v. Kohler Co.*, 2022 WI 52, ¶ 18, 977 N.W.2d 342. Like federal courts, Wisconsin courts require that the plaintiff allege an "injury-in-fact"—one that is "neither hypothetical nor conjectural." *Id.*, ¶ 21; *c.f. City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (a federal plaintiff must show a "real and immediate," not "conjectural" or "hypothetical" injury or threat of injury).

The Wisconsin Court of Appeals in *Bauer* rejected the reasoning of *Remijas* and *Lewert* and concluded that the plaintiffs—alleging only a data breach and no identity theft—had not alleged an "actual" injury. *Bauer*, 2025 WL, ¶ 27 (quoting *Tietsworth v. Harley-Davidson, Inc.*, 2004 WI 32, ¶ 17, 677 N.W.2d 233 ("Actual damage is harm that has already occurred or is 'reasonably certain' to occur in the future. Actual damage is not the mere possibility of future harm."). Rather, it concluded that

> "[T]he risk of future harm and the actions taken to protect against that risk, as alleged by the Employees in this case, remain too attenuated and speculative to confer standing to pursue their claims, absent a demonstration that identity theft or data misuse has already occurred. Without allegations of any previous identity theft or data misuse suffered by themselves or any other members of the class, the employees have failed to allege sufficiently imminent or certainly impending future injury."

Bauer, 2025 WL, ¶ 27. While this directly conflicts with my standing decision above—and decisions of the Seventh Circuit that are binding upon me but not the Wisconsin Court of

Appeals—it is instructive as to how the Wisconsin courts would rule on the negligence injury element in this case.

Recall that a plaintiff in Wisconsin must allege "actual loss or damage resulting from the injury" to state a claim for negligence. *Gritzner*, 2000 WI, at ¶ 19. As a federal court, I must try my best to guess how the state judiciary would rule on an ambiguous question of state law. *Green Plains Trade Group, LLC v. Archer Daniels Midland Co.*, 90 F.4th 919, 927–28 (7th Cir. 2024). This includes giving significant weight to the opinions of intermediate appellate courts. *Id.* at 928. If the most recent Wisconsin appellate court to consider these facts—a data breach with no alleged identity theft—has concluded that no actual or imminent injury occurred, albeit in the standing context, it is hard to imagine that they would find "harm that has already occurred or is reasonably certain to occur in the future," "not the mere possibility of future harm," when considering the injury element of negligence. *Hennekens,* 160 Wis.2d at 152–53 (cleaned up). Although *Reetz* directly addressed the elements of negligence, I find *Bauer* more instructive because it is more recent and more factually analogous to this case. Therefore, I conclude that plaintiff has not stated a claim as to negligence under Wisconsin law.

C. California Consumer Privacy Act (CCPA)

Defendant argues that plaintiff has not stated a claim under the California Consumer Privacy Act ("CCPA"). Cal. Civ. Code § 1798.150. That law allows "[a]ny consumer whose nonencrypted and nonredacted personal information . . . or whose email address in combination with a password or security question and answer would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the

information to protect the personal information may institute a civil action[.]" Cal. Civ. Code § 1798.150(a)(1). To state a claim, therefore, the plaintiff must allege that his or her personal information was taken as a result of the business's failure to implement and maintain reasonable security practices and procedures appropriate to the nature of the information. *Id.*

Defendant argues that plaintiff's allegations on this count are conclusory, while plaintiff argues that they are sufficient. Plaintiff points to paragraphs 36 and 49 of the amended complaint as most responsive:

> Prior to the Data Breach Incident, Defendant should have ensured that it had adequate monitoring software in place to detect intrusions or the transfer of large volumes of data to third party networks, that it implemented multi-factor authentication to verify the credentials of individuals attempting to access Private Information, that it limited access to Private Information to only necessary employees, that it encrypted or tokenized Private Information in internet accessible locations, and that it deleted or redacted Private Information that it was no longer required to maintain. By failing to implement these reasonable and industry standard data security measures, Defendant left Plaintiff's and Class members' Private Information in a condition vulnerable to unauthorized access.

(Am. Compl. ¶ 36.)

> Despite knowing the prevalence of data breaches, Defendant failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly sensitive systems and databases. Defendant could have prevented the Data Breach by encrypting and/or redacting sensitive data, limiting access to Private Information to only necessary employees, monitoring their network for signs of intrusion or the transfer of large volumes of data, and employing multi-factor authentication to ensure that only authorized individuals are granted access to sensitive data.

(*Id.* ¶ 49.) One California district court notes that "[c]ourts are split on what is required to adequately plead that a defendant failed to maintain reasonable security procedures." *Little Seeds Children's Center, Inc. v. Citybank, N.A.*, 25-cv-1517-hsg, 2025 WL 3141496, *8 (N.D. Cal. Nov. 10, 2025). Some courts demand specific allegations of "how or why [the defendant] knew or should have known its systems were inadequate or unreasonable." *Griffey v. Magellan Health Inc.*, 562 F.Supp.3d 34, 57 (D. Ariz. 2021). Others recognize that the plaintiff

will often have few details of the defendant's cybersecurity practices at the pleading stage and so are willing to draw more generous inferences. *See Doe v. MKS Instruments, Inc.*, No. SACV 23-868-CJC, 2023 WL 9421115, *3 (C.D. Cal. Nov. 3, 2023).

Taking as true the allegations in paragraphs 36 and 49 of the amended complaint, I find that plaintiff has sufficiently alleged a claim under Cal. Civ. Code § 1798.150(a)(1). Plaintiff's allegations go beyond a threadbare recital of the elements as required under *Iqbal* and *Twombly*. *Iqbal*, 556 U.S. at 678. The complaint alleges several plausibly reasonable and common cybersecurity measures that defendant did not use: monitoring software, multi-factor credential authentication, limited employee access, encryption or tokenization on systems exposed to internet traffic, and periodic deletion of data. Accepting as true that defendant was aware of these practices, they were reasonable for defendant's business and the nature of the data it held, and one or more of them would have prevented the October 18, 2024, breach, the complaint is sufficient to proceed beyond the pleading stage.

D. California Unfair Competition Law (UCL)

Defendant first argues that plaintiff's claim under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, should be dismissed because defendant is a Wisconsin company, the alleged wrongdoing occurred outside of California, and California's UCL therefore does not impose liability. Defendant cites the California decision *Sullivan v. Oracle Corp.* which held that a "presumption against extraterritoriality applies to the UCL in full force." 254 P.3d 237, 248–49 (Cal. 2011) (holding that UCL "does not apply to overtime work performed outside California for a California-based employer by out-of-state plaintiffs"). This presumption should apply unless an intention to apply outside of California "is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history." *Id.* Plaintiff countered by stating that some courts have permitted UCL claims by California residents for misconduct occurring out-of-state. *See In re MOVEit*

Customer Data Security Breach Litigation, No. 23-md-3083, 2025 WL 2176590, *23 (D. Mass. July 31, 2025) ("[A] UCL claim may be brought by a plaintiff who is a resident of California, regardless of where the alleged misconduct occurred.") (quoting *Adobe Sys. Inc. v. Blue Source Grp., Inc.*, 125 F. Supp. 3d 945, 972 (N.D. Cal. 2015). Digging deeper, the *Adobe* decision cites to two earlier California decisions: *Norwest Mortgage, Inc. v. Superior Court*, 72 Cal.App.4th 214, 222, 85 Cal.Rptr.2d 18 (1999), and *Yu v. Signet Bank/Virginia*, 69 Cal.App.4th 1377, 1391–92, 82 Cal.Rptr.2d 304 (1999)).

The case that plaintiff cites, and the bright-line rule it pulled from *Adobe* and other cases in that line, seems to oversimplify the issue. As another court in this circuit found, that line from *Adobe* was not the product of "any substantive analysis of the extraterritorial reach of the Unfair Competition Law." *Elzeftawy v. Pernix Group, Inc.*, 477 F. Supp. 3d 734, 785 (N.D. Ill. 2020). The *Norwest* decision involved a California company defendant where the alleged misconduct had a direct California connection. *Id.* (citing *Norwest Motgage, Inc.*, 85 Cal.Rptr.2d at 20). As to *Yu*, it stated that the decision "does not stand for the proposition that a UCL claim may survive against an out-of-state defendant, based on out-of-state conduct, *solely* because the plaintiff is a California resident; rather, the defendant must be subject to personal jurisdiction in California, too." *Id.* "[N]either *Norwest* nor *Yu* stands for the proposition that the UCL automatically applies to *any* claim brought by a California resident." *Id.* As the *Elzeftawy* court concluded, and defendant similarly argues, the applicability of California's UCL to out-of-state defendants must hinge on whether plaintiff's claim "'would cause it to operate, impermissibly, with respect to occurrences outside' California." *Id.* (citing *Sullivan*, 254 P.3d at 248). In other words, the extraterritoriality of a UCL remedy must be determined in light of the "liability-creating conduct," where liability is defined by the underlying law—in this case, the CCPA. *See Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018). To make this determination, I consider the connections between the alleged misconduct, the

State of California, and the intent behind the law at issue. *See id.* I also consider whether applying California law would displace another state's analogous law, or rather, whether not applying California law would leave some plaintiffs with no comparable remedy under other state's laws. *Id.* My focus is on the extraterritorial intent of the underlying legal duty, as the UCL operates by "borrowing" legal duties from other laws and providing a remedy when they are violated. *Rose v. Bank of America, N.A.*, 304 P.3d 181, 185, 57 Cal.4th 390 (Cal. 2013).

Plaintiff alleged that defendant violated the California UCL by engaging in an "unlawful" business practice by violating the CCPA. I found above that plaintiff had stated a claim under the CCPA. While it is well-settled that "[t]he UCL does not apply to actions occurring outside of California that injure non-residents" of California, plaintiff has expressly limited his UCL claim to the subclass of California residents of which he is a member. *Campbell v. Honey Science, LLC*, __ F. Supp. 3d __, 2025 WL 3454836, *2 (N.D. Cal. 2025).

By my research, at least one court has applied the UCL to non-California defendants where the plaintiff is a California resident by concluding that the CCPA was intended to apply extraterritorially to protect California residents. *Sanchez v. Xavier U. of La.*, No. 23-cv-1269, 2024 WL 4251906, *10 (E.D. La. Jul. 18, 2024). As that court notes, California law by its plain language applies to "[a] business that owns, licenses, or maintains personal information about a California resident." Cal. Civ. Code § 1798.81.5. It also suggests that the CCPA should operate alongside, rather than displace, other state or federal laws to ensure a minimum level of protection for California residents. Cal. Civ. Code § 1798.81.5(e)(5). Given the nature of interstate commerce, it seems unlikely that California lawmakers intended for a consumer protection law to apply only against California businesses. The language of CCPA evinces an intent to protect California residents from negligent data security practices regardless of where the businesses holding their data are located. This intent is sufficient to overcome

whatever presumption against extraterritoriality might exist; therefore, I find that defendant's extraterritoriality argument is without merit.[2]

Defendant next argues that plaintiff's UCL claim fails because he did not suffer "lost money or property." Cal. Bus. & Prof. Code § 17204. California courts have read this to require some economic injury "such as surrendering more or acquiring less in a transaction, having a present or future property interest diminished, being deprived of money or property, or entering a transaction costing money or property that would otherwise have been unnecessary." *R.C. v. Walgreen Co.*, 733 F. Supp. 876, 903 (C.D. Cal. 2024) (citing *Kwikset Corp v. Superior Court*, 51 Cal.4th 310, 246 P.3d 877 (2011)). Plaintiff argues that the diminished value of his private information, "monetary damages from fraud and identity theft," and "time and expenses related to monitoring [his] financial accounts for fraudulent activity" qualify under a broader reading. ECF No. 11 at 11–12 (citing *In re MOVEit Customer Data Security Breach Litigation*, 2025 WL 2176590, at *23).

I disagree with defendant and find that plaintiff has alleged a sufficient injury under the UCL. Plaintiff has not alleged he suffered actual identity theft or that he entered a transaction, perhaps with a data monitoring service, that he would not have otherwise done.[3] Plaintiff has alleged, however, that he failed to receive the "benefit of their bargain" by overpaying for services "that should have included data security but did not," as well as the diminished value of his personal information and his own personal time reviewing his financial accounts for signs of fraud. (Am. Compl. ¶ 137.) Like in the Article III context, California courts do not view

[2] I find the cases defendant cites which reach the opposite conclusion to be unpersuasive. For instance, *Toretto* correctly identifies caselaw discussing the UCL itself but focuses entirely on the location of the alleged harm rather than ask whether the presumption against extraterritoriality has been rebutted. *Toretto v. Donnelley Financial Solutions, Inc.*, 583 F. Supp. 3d 570, 604–05 (S.D.N.Y. 2022).

[3] In fact, defendant offered plaintiff a free one-year subscription to a credit monitoring service, but plaintiff refused to use it as he "does not trust Defendant's chosen vendor," but he has not alleged to have purchased an alternative service with his own money. (Am. Compl. ¶ 21.)

personal information to be cognizable as property for UCL purposes. *See Hart v. TWC Product & Tech. LLC*, 526 F. Supp. 3d 592, 603 (N.D. Cal. 2021) ("That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property."); *see also Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018) ("[T]he sharing of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing purposes."). Therefore, the diminution in value of his personal information could not serve to establish UCL standing.

It is less clear whether the mere loss of personal time in monitoring his financial accounts qualifies as a loss of "money or property," although that seems dubious under a plain reading of those words. What is clear, however, is that plaintiff's benefit-of-the-bargain theory is sufficient under the UCL. Plaintiff claims that he (or his employer vis-à-vis his compensation which includes health care benefits) paid more for his health insurance than he otherwise would have had he known they had inadequate data security, or received less than the implied secure treatment of his data he expected. (Am. Compl. ¶ 137.) This theory has been endorsed by California courts in pleading a UCL claim:

> Here, appellants alleged they relied on Centrelake's false representations and promises concerning data security in entering contracts with Centrelake and accepting its pricing terms, paying more than they would have had they known the truth that Centrelake had not implemented and would not maintain adequate data security practices. We conclude these allegations adequately pleaded UCL standing under *Kwikset*.

Moore v. Centrelake Medical Group, Inc., 83 Cal.App.5th 515, 527–28, 299 Cal.Rptr.3d 544 (2022) (citing *Kwikset*, 246 P.3d 877 (2011)). Therefore, plaintiff has alleged that he has lost money or property as the UCL requires.

Finally, defendant argues that plaintiff has not alleged that he lacks an adequate remedy at law. Even where state law permits state courts to employ equitable remedies in

non-traditional ways, equitable jurisdiction under federal common law "remains cabined to the traditional powers exercised by English courts of equity, even for claims arising under state law." *Sonner v. Premier Nutrition Corp*., 971 F.3d 834, 840 (9th Cir. 2020). (citing *Guarantee Trust Co. of New York v. York*, 326 U.S. 99, 112 (1945)). In federal court, a plaintiff must establish that he lacks "an adequate remedy at law before securing equitable restitution for past harm under the UCL . . ." *Id.* And equitable remedies such as injunctions, restitution, and civil penalties are the only remedies available under California's UCL. *Adir Int., LLC v. Starr Indem. & Liab. Co.*, 994 F.3d 1032, 1043 (9th Cir. 2021).

I find that plaintiff has not adequately pled that he lacks an adequate remedy at law. Recall that I permitted plaintiff's CCPA claim to proceed as to past harm—undoubtedly an adequate remedy—and that plaintiff's claims for future harm (money, injunctive, and declaratory) were all dismissed for lack of Article III standing. Therefore, I lack equitable jurisdiction to entertain plaintiff's UCL claim.

E. California Confidentiality of Medical Information Act (CMIA)

Finally, defendant argues that plaintiff failed to state a claim under California's Confidentiality of Medical Information Act (CMIA). Defendant first points out that any of defendant's liability under CMIA must arise from Cal. Civ. Code § 56.26(a) rather than § 56.10(a), as defendant is a third-party benefit administrator rather than a "provider of health care, health care service plan, or contractor." § 56.10(a). Plaintiff alleged in the amended complaint that defendant is a "contractor," and alternatively alleged that defendant is a "provider of health care" because it is a "business organized for the purpose of maintaining medical information [and providing that information upon request]" or a "business that offers software or hardware to customers . . . in order to make the information available to an individual or a provider of health care. . ." Cal. Civ. Code § 56.06(a–b); (Am. Compl. ¶ 142.)

Defendant concedes that, as a third-party administrator, it is covered by Cal. Civ. Code § 56.26(a) as an "entity engaged in the business of furnishing administrative services to programs that provide payment for health care services." This statute requires that the defendant "knowingly use, disclose, or permit its employees or agents to use or disclose medical information . . . except as reasonably necessary in connection with" the administrative purpose of the program. § 56.26(a).

I find that it is premature to decide what sort of entity defendant is for the purpose of CMIA liability. Accepting as true plaintiff's allegations that defendant is either a "contractor," a "business organized for the purpose of maintaining medical information," or a "business that offers software of hardware to consumers" to maintain medical information, defendant's dispute is better suited for summary judgment where I may consider evidence outside the pleadings. From the four corners of the complaint, I find it to be plausible that defendant is one of those three entities.

Finally, I agree with defendant that plaintiff's allegation that "medical information" was leaked is conclusory and does not state a claim. (Am. Compl. ¶ 124.) While I admit that it may be difficult for plaintiff to know what information was lost before the discovery phase, I must enforce the rule that allegations must be non-conclusory and sufficient to state a claim that is plausible. Courts have demanded more than merely alleging the loss of medical information within the meaning of Civil Code § 56.05(j), as this is nothing more than an element of the cause of action. *See Strong v. LifeStance Health Group Inc.*, No. cv-23-682, 2025 WL 317552, *10–11 (D. Ariz. Jan. 28, 2025); *Wilson v. Rater8, LLC*, No. 20-cv-1515, 2021 WL 4865930, *5 (S.D. Cal. Oct. 18, 2021); *see also Iqbal*, 556 U.S. at 663. As these cases show, not all personal information constitutes medical information under CMIA, and it is plaintiff's burden to allege facts showing it is plausible that the correct type of data was leaked. Plaintiff has not, therefore he has not stated a claim under CMIA.

IV. CONCLUSION

Plaintiff's first amended complaint has sufficiently alleged standing as to past harm, but not future harm. Plaintiff has stated a claim as to the California Consumer Privacy Act (CCPA), but not the California Unfair Competition Law (UCL), California Confidentiality of Medical Information Act (CMIA), or common law negligence. Therefore, **IT IS ORDERED** that defendant's Motion to Dismiss for Lack of Subject-Matter Jurisdiction is **GRANTED IN PART** and **DENIED IN PART**. Defendant's Motion to Dismiss for Failure to State a Claim is **GRANTED IN PART** and **DENIED IN PART**.

I will grant plaintiff leave to amend his complaint. Plaintiff may file a second amended complaint no later than **February 18, 2026**. If plaintiff does not file an amended complaint, defendant shall answer the first amended complaint no later than **March 4, 2026**.

Dated at Milwaukee, Wisconsin, this 27th day of January, 2026.

/s/ Lynn Adelman
LYNN ADELMAN
United States District Judge