UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION	*	
This Order Relates to the Following Cases:	*	MDL No. 23-md-3083-ADB-PGL
PROGRESS BELLWETHER CASES ONLY.	*	

MDL Order No. 23

(Direct User and VCE/VCEC Motions to Dismiss for Failure to State a Claim)

BURROUGHS, D.J.

Defendants Pension Benefit Information LLC ("PBI"); Genworth Financial, Inc., Genworth Life and Annuity Insurance Company, Genworth Life Insurance Company, (collectively, "Genworth"), Teachers Insurance and Annuity Association of America ("TIAA"), Milliman Solutions, LLC, Milliman Inc., (collectively, "Milliman"), and Members Life Insurance Company ("MLIC") (all collectively, the "PBI Bellwether Defendants"); Delta Dental of California, in combination with affiliate insurers in other states named as Defendants in the Corrected Bellwether Consolidated Class Action Amended Complaint ("CAC") (collectively "Delta Dental Bellwether Defendants" or "Delta Dental"); Maximus, Inc., along with its subsidiaries Maximus Federal Services, Inc., Maximus Human Services, Inc., and Maximus Health Services, Inc., (collectively "Maximus Bellwether Defendants" or "Maximus"); and Welltok, Inc.; Corewell Health, Sutter Health, OSF Healthcare System, CHI Health - NE, and Virginia Mason Franciscan Health (collectively with Welltok, Inc., "the Welltok Bellwether Defendants") (all collectively, "Defendants"), move to dismiss the allegations against them contained in Chapters One and Three through Six of the CAC [ECF No. 1332 (the "Bellwether

Complaint" or "CAC")], on the ground that Plaintiffs have failed to state a claim under Federal Rule of Civil Procedure 12(b)(6). See [ECF Nos. 1359 ("PBI Mot."), 1370 ("Delta Dental Mem."), 1371 ("Maximus Mot."), 1377 ("Welltok Mem.")]. Having reviewed the Bellwether Complaint, Defendants' memorandums in support of their motions, see [Delta Dental Mem.; Welltok Mem.; ECF Nos. 1360 ("PBI Mem."), 1371-1 ("Maximus Mem.")]; Plaintiffs' oppositions [ECF Nos. 1438 ("Maximus Opp."), 1440 ("Delta Dental Opp."), 1441 ("Welltok Opp."), 1442 ("PBI Opp.")]; Defendants' replies [ECF Nos. 1465 ("Welltok Reply"), 1467 ("PBI Reply"), 1468 ("Maximus Reply"), 1470 ("Delta Dental Reply"),], and the exhibits accompanying the parties' filings, the Court hereby orders that:

- The PBI Bellwether Defendants' motion is **GRANTED** on Counts 3–4, 7, 9, 11, 12, 14, 15–17, 19–27; **GRANTED IN PART** on Count 2, **DENIED** on Counts 1, 5–6, 8, 10, 13, 18, and 28.
- The Delta Dental Bellwether Defendants' motion is **GRANTED** on Counts 2, 3–9, 11, 13–14, 16–17, 20, and 24–25; **GRANTED IN PART** on Counts 17–18, and **DENIED** on Counts 1, 10, 12, 15, 17, 19, 23, and 26.
- The Maximus Bellwether Defendants' motion is **GRANTED** on Counts 5–9, 12, 14–15, and 17–19; **GRANTED IN PART** on Count 3, and **DENIED** on Counts 1–2, 4, 10–11, 13, and 16.
- The Welltok Bellwether Defendants' motion is **GRANTED** on Counts 4–5, 9, 11–15, 17, and 21; **GRANTED IN PART** on Count 2, and **DENIED** on Counts 1, 3, 6–8, 10, 16, 18–20, and 22.

Plaintiffs' allegations and claims against the Progress Defendants are the subject of MDL Order No. 22.

I. Background

a. Key Facts

The following reflects the well-pleaded allegations set forth in the Bellwether Complaint. See Ocasio-Hernández v. Fortuño-Burset, 640 F.3d 1, 5 (1st Cir. 2011).

i. MOVEit Transfer and the Data Breach

MOVEit Transfer is an encrypted file-transfer software offered by Progress Software Corporation, based in Burlington, Massachusetts. [CAC ¶¶ 6, 918, 966]. The software applies encryption protocols to secure users' data both while it is being transferred and while it is being stored. [Id. ¶ 969]. These protocols are "virtually unbreakable with existing technology," [id. ¶¶ 970–71], meaning that under ordinary circumstances, files encrypted by MOVEit "can only be read if the user has the appropriate encryption keys, even if the files are stolen," [id. ¶ 969].

The software "is licensed to customers on a subscription basis and installed by customers on their own servers." [CAC ¶ 967]. Then, "users—such as the customer's employees—access the software through a MOVEit Transfer software client installed on a computer, phone, or a website accessible over the Internet that connects to the customer's MOVEit Transfer server."[1] [Id. ¶ 973]. Progress provides security and software support, including "bug fixes, patches, upgrades, enhancements, new releases [and] technical support," to MOVEit Transfer customers. [Id. ¶ 972].

On May 27, 2023, a Russian ransomware group called CL0P "deploy[ed] malware to public-facing MOVEit Transfer web portals" that allowed the hackers to decrypt and download

[1] Customers "can also access MOVEit Transfer through a REST API, a programmatic means of interacting with the MOVEit Transfer server without using a graphical user interface such as a client or website." [CAC ¶ 975].

data stored in the MOVEit software (the "Data Breach"). [CAC ¶ 14]. By doing so, CL0P was able to exfiltrate personally identifiable information ("PII") and, in some cases, protected health information ("PHI") from more than 2,600 entities, affecting more than 93 million individual records as of January 2024. [Id. ¶¶ 1, 19, 1164, 1175].

CL0P's malware exploited three vulnerabilities in MOVEit Transfer—SQL injection, .NET BinaryFormatter deserialization, and unencrypted MOVEit's decryption keys, [CAC ¶¶ 996–1056]—which were endemic to the code of "[a]ll versions of MOVEit Transfer," [Id. ¶ 1112]. Progress's technical support teams began receiving reports of suspicious activity the next day. [Id. ¶ 1125]. On June 5, 2023, "multiple companies began coming forward to announce that their MOVEit Transfer servers [had been] compromised." [Id. ¶ 1132]. By that time, Microsoft had attributed the Data Breach to CL0P. [Id. ¶ 1156]. CL0P then claimed public credit for the Data Breach and, on June 6, 2023, "threatened to post stolen user data online unless the compromised organizations paid a ransom." [Id. ¶¶ 1157–58]. In the months that followed, CL0P published the names of entities from which it had stolen data through the Data Breach, eventually naming more than 2,600 companies or other entities. [Id. ¶¶ 1159–64]. Plaintiffs also allege that CL0P has made good on its threat to post users' information on the dark web and elsewhere, and that such disclosure has caused them to suffer an array of legally cognizable injuries, discussed further below. [Id. ¶¶ 1157, 1193, 1199–211].

ii. Bellwether Defendants

1. PBI Bellwether Defendants

PBI is a Minnesota-based corporation, [CAC ¶ 927], that performs "data verification, death audit, and participant location services" for insurance companies, pension funds, and other similar organizations, [id. ¶ 1831]. Several of PBI's clients—Genworth, GLAIC, GLIC, TIAA,

Milliman, and MLIC—are part of the current bellwether litigation. [Id. ¶ 1823]. To perform services for those clients, PBI solicited data about its clients' customers, which it received and stored via an administrative portal that utilized MOVEit Transfer. [Id. ¶¶ 1835, 1839–40].

2. Delta Dental Bellwether Defendants

Delta Dental of California, in combination with affiliate insurers in other states named as defendants in the CAC, is a nationwide dental insurance provider. [CAC ¶¶ 2404–14]. Delta Dental uses MOVEit Transfer to share information among its affiliates. [Id. ¶¶ 2418, 2424–25]. The Delta Dental Bellwether Defendants entered into Business Associate Agreements ("BAAs") pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") among themselves and with Progress in order to transfer customers' personal health information ("PHI") and other insurance information via MOVEit. [Id. ¶¶ 2424–26].

3. Maximus Bellwether Defendants

Maximus, Inc., along with its subsidiaries Maximus Federal Services, Inc., Maximus Human Services, Inc., and Maximus Health Services, Inc., is a government contractor that helps state and federal agencies administer benefits programs, including Medicare and Medicaid. [CAC ¶¶ 2931–32]. "Maximus provides medical evaluations, review of eligibility appeals, enrollment assistance, data analysis, and IT and consulting services." [Id. ¶ 2932]. To receive those services, Maximus's clients share private information relating to benefits applicants or recipients. [Id. ¶¶ 2934–35]. "Maximus uses MOVEit for internal and external file sharing purposes, including to share data with government customers related to Maximus's services in support of certain government programs." [Id. ¶ 2936].

4. Welltok Bellwether Defendants

Welltok, Inc. is a Rhode Island-based corporation, [CAC ¶ 939], that helps healthcare and insurance providers incentivize their customers to take steps to improve their health, such as by getting vaccines or other preventative care, [id. ¶¶ 3300–01]. Welltok's service analyzes its clients' patient or policyholder data to draw predictive inferences about how to nudge consumers toward certain health choices. [Id. ¶¶ 3303–04]. Welltok interacted with its clients via a consumer-activation platform that utilized MOVEit Transfer to communicate and store sensitive information. [Id. ¶¶ 3310–11]. As relevant here, Welltok provided customer-activation services to Sutter Health, OSF Healthcare System ("OSF"), Corewell Health ("Corewell"), CHI Health – NE ("CHI"), and Virginia Mason Franciscan Health ("Virginia Mason") (together, the "Welltok VCE Defendants"). [Id. ¶¶ 3311–17]. In the course of providing those services, Plaintiffs allege that the Welltok VCE Defendants transferred their private information to Welltok via Welltok's MOVEit Transfer server. [Id.]. Such data varied by Defendant, but included names, addresses, dates of birth, clinical information, patient IDs, and health insurance information. [Id.] Plaintiffs also allege that Corewell and OSF transferred their social security numbers via Welltok's MOVEit Transfer server. [Id. at ¶¶ 3312–13].

iii. Alleged Failure to Prevent the Data Breach

Plaintiffs allege that the non-Progress Bellwether Defendants could have, and failed to, prevent the data breach if it had properly used and implemented industry standard cybersecurity techniques and protocols. [CAC ¶ 1291]. Plaintiffs' allegations fall into two categories that correspond to the nature of each Defendants' interactions with MOVEit.

First, Plaintiffs allege that the "direct users" of MOVEit—PBI, Welltok, Delta Dental, and Maximus, each of whom contracted with Progress to set up a MOVEit Transfer interface on

their own servers—failed to implement security protocols that would have prevented the Data Breach. See [CAC ¶¶ 1977–95 (PBI); id. ¶¶ 2492–2513 (Delta Dental); id. ¶¶ 2974–90 (Maximus); id. ¶¶ 3424–45 (Welltok)]. The allegedly omitted security practices included:

- auditing the security of the MOVEit Transfer software, e.g., [id. ¶ 1977];
- auditing Progress's cybersecurity practices, e.g., [id. ¶ 1978];
- restricting the IP addresses that could access the MOVEit Transfer interface ("whitelisting"), e.g., [id. ¶ 1979];
- limiting the file types that could be uploaded to MOVEit Transfer, e.g., [id. ¶¶ 1980–81];
- implementing logging and monitoring programs that might have detected CL0P's intrusion before it executed harmful code, e.g., [id. ¶¶ 1982–87].

Some of these, including audit logging and whitelisting, are recommended by Progress and are configurable within the MOVEit software interface. [Id. ¶¶ 2002–08]. Plaintiffs contend that these configurations would have prevented the SQL injection and LEMURLOOT malware execution attack that CL0P perpetrated. [CAC ¶¶ 1980, 2513, 2977, 2990, 3432, 3445].

Plaintiffs allege a separate set of failures against the direct users' clients (e.g., Genworth, TIAA, Corewell, etc., whom the parties refer to collectively as "vendor contracting entities" or "VCEs"). See generally [CAC]. Plaintiffs assert that the VCEs failed to implement vendor-management systems to properly vet and audit vendors before sharing data with them. [CAC ¶ 2014 (PBI VCEs)]; [id. ¶ 3464 (Welltok VCEs)].

b. Procedural History

After extensive negotiation among the parties, the Court ordered bellwether proceedings in this case, and agreed that the Plaintiffs could consolidate and amend their allegations in the CAC in due course. Plaintiffs filed an initial amended Bellwether Complaint on December 6, 2024, see [ECF No. 1297], which they corrected on January 9, 2025 with Defendants' stipulated

consent, see [ECF No. 1331 (stipulation)]; [ECF No. 1332 ("CAC")].[2] The CAC names Progress, as well as the PBI Bellwether Defendants, Delta Dental, Maximus, and the Welltok Bellwether Defendants (together, the "non-Progress Defendants").

The non-Progress Defendants moved to dismiss on February 4, 2025, [PBI Mot., Delta Dental Mem., Maximus Mot., Welltok Mem.], Plaintiffs opposed on April 7, 2025, [ECF No. 1438 ("Maximus Opp."); ECF No. 1440 ("Delta Dental Opp."); ECF No. 1441 ("Welltok Opp."); PBI Opp.], and the non-Progress Defendants replied on April 28, 2025, [PBI Reply; Maximus Reply, Delta Dental Reply, Welltok Reply]. Progress moved for dismissal on the same timeline, and its motion is the subject of MDL Order No. 22, filed contemporaneously with this order. The Court held oral argument on May 12, 2025.

II. Legal Standard

a. Rule 12(b)(6) Motion to Dismiss

Except for claims governed by Federal Rule of Civil Procedure 9(a), see infra, "[d]ismissal of a complaint pursuant to Rule 12(b)(6) is inappropriate if the complaint satisfies Rule 8(a)(2)'s requirement of a 'short and plain statement of the claim showing that the pleader is entitled to relief.'" Ocasio-Hernández, 640 F.3d at 11–12 (quoting Fed. R. Civ. P. 8(a)(2)). "A short and plain statement needs only enough detail to provide a defendant with fair notice of what the . . . claim is and the grounds upon which it rests." Id. at 12 (internal quotation marks omitted) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007)). Still, "in order to 'show' an entitlement to relief a complaint must contain enough factual material 'to raise a right to relief above the speculative level on the assumption that all the allegations in the complaint are true (even if doubtful in fact).'" Id. (quoting Twombly, 550 U.S. at 555). "Where a complaint

[2] References to the Bellwether Complaint or the CAC refer to the corrected version.

pleads facts that are 'merely consistent with' a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." Id. (internal quotation marks omitted) (quoting Ashcroft v. Iqbal, 556 U.S. 662, 670 (2009)).

To apply these standards, the Court "employ[s] a two-pronged approach." Ocasio-Hernández, 640 F.3d at 12. To begin, it must "identify[] and disregard[] statements in the complaint that merely offer 'legal conclusions[s] couched as . . . fact[]' or '[t]hreadbare recitals of the elements of a cause of action.'" Id. (first and second alterations added) (quoting Iqbal, 556 U.S. at 678). "Non-conclusory factual allegations in the complaint must then be treated as true, even if seemingly incredible." Id. "If that factual content, so taken, 'allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged,' the claim has facial plausibility." Id. (quoting Iqbal, 556 U.S. at 663). The resulting inquiry demands a "context-specific" approach, asking the Court "to draw on [its] judicial experience and common sense." Iqbal, 556 U.S. at 679.

a. Rule 9(b) Heightened Pleading

For claims sounding in fraud, and, as relevant here, claims alleging fraudulent misrepresentation, Federal Rule of Civil Procedure 9(b)'s special pleading requirements apply. Rule 9(b) states that "a party must state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). The First Circuit interprets this standard as requiring parties to set out "the who, what, where, and when of the allegedly false or fraudulent representation," Alt. Sys. Concepts, Inc. v. Synopsys, Inc., 374 F.3d 23, 29 (1st Cir. 2004), and specify "the basis for inferring scienter," Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd., 419 F. Supp. 3d 176, 189 (D. Mass. 2019) (quoting N. Am. Cath. Educ. Programming Found., Inc. v. Cardinale, 567 F.3d 8, 13 (1st Cir. 2009)). In misstatement cases, "the specificity requirement extends only

to the particulars of the allegedly misleading statement itself. The other elements of fraud, such as intent and knowledge, may be averred in general terms." Rodi v. S. New Eng. Sch. of L., 389 F.3d 5, 15 (1st Cir. 2004) (citations omitted); see also Runyon v. Wellington Mgmt. Co., LLP, No. 13-cv-11236, 2015 WL 1276825, at *5 (D. Mass. Mar. 20, 2015) (noting that "reliance" is not subject to Rule 9(b)'s heightened pleading requirement).

III. Discussion

This opinion addresses the claims of dozens of plaintiffs against four groups of defendants, and therefore necessarily covers a myriad of topics. First, the Court will address the personal jurisdiction issues raised by the PBI Bellwether Defendants and Maximus. Next, the Court will address Plaintiffs' common law claims, including the choice of law analysis. Finally, the Court will turn to Plaintiffs' statutory claims under the relevant state law.

a. Personal Jurisdiction

The PBI Bellwether Defendants and Maximus assert that certain of the forums lack personal jurisdiction over them with respect to particular plaintiffs' claims. Plaintiff Barbara Cruciata, a New York and Florida resident, sues Maximus, a Virginia-based corporation, in the District of Massachusetts, which Maximus contests based on a lack of personal jurisdiction. See [Maximus Mem. at 29]. The PBI Bellwether Defendants also assert jurisdictional defects. Genworth (headquartered in Virginia) and TIAA (headquartered in New York) assert they should not be subject to general or specific personal jurisdiction in Minnesota or Massachusetts, where they face claims from Plaintiffs Camille and Eugene Burgan (Massachusetts), Margaret Phelan (Minnesota), and Tricia Hernandez (Minnesota). [PBI Mem. at 84]. MLIC (headquartered in Iowa) asserts that it should not be subject to personal jurisdiction in the Western District of Washington, where it faces claims by Plaintiff Jose Soto. [Id.] And PBI (headquartered in

Minnesota) contests personal jurisdiction in Massachusetts, Virginia, Washington, New York, and Illinois. [Id.]

Plaintiffs do not dispute the lack of general personal jurisdiction over Defendants in the foregoing jurisdictions, but maintain that the relevant courts may act based on specific jurisdiction. [Maximus Opp. at 26; PBI Opp. at 81]. Thus, the Court evaluates in turn whether Maximus should be subject to personal jurisdiction in Massachusetts; whether Genworth should be subject to personal jurisdiction in Massachusetts; whether MLIC should be subject to personal jurisdiction in Washington; whether Genworth and TIAA should be subject to personal jurisdiction in Minnesota; whether PBI should be subject to personal jurisdiction in Massachusetts, Virginia, Washington, New York, or Illinois.

First, Plaintiffs offer no argument why Genworth should be subject to personal jurisdiction in Massachusetts, or why MLIC should be subject to jurisdiction in Washington. The Court deems these arguments abandoned and finds personal jurisdiction lacking as to such claims.

Second, Plaintiffs contend that Genworth and TIAA are subject to personal jurisdiction in Minnesota. PBI is located in Minnesota and thus subject to general jurisdiction in the state, and—Plaintiff's argue—because Genworth and TIAA transferred Plaintiffs' data to PBI, Genworth and TIAA are subject to personal jurisdiction in Minnesota.[3] [PBI Opp. at 64]. The problem is that the CAC, as Plaintiffs assert in their opposition to Progress, does not contain any factual allegations concerning the location of PBI's (or any other direct users') servers. See [ECF No. 1437 ("Progress Opp.") at 28]. The only concrete connection linking Genworth and

[3] Minnesota's long-arm statute is coextensive with federal due process. Custom Conveyor Corp. v. Hyde, 237 F. Supp. 3d 895, 898 (D. Minn. 2017).

TIAA to Minnesota is their business relationship with PBI. There is no allegation that any of Genworth or TIAA's conduct which gave rise to Plaintiffs' claims occurred in Minnesota, as opposed to Virginia and New York. See Bristol-Myers Squibb Co. v. Superior Ct., 582 U.S. 255, 265 (2017) ("What is needed . . . is a connection between the forum and the specific claims at issue."). The Court thus concludes that personal jurisdiction is also lacking as to Plaintiff Phelan's claims against TIAA and Plaintiff Hernandez's claims against Genworth in Minnesota.

Third, Plaintiffs contend that PBI is subject to personal jurisdiction in Massachusetts, Virginia, Washington, New York, and Illinois for claims brought by non-residents of those states. [PBI Opp. at 82]. Plaintiffs argue that there is jurisdiction because Plaintiffs' "relationship[s]" to the breach stemmed from these cases. [Id.] For example, they allege that one plaintiff brought suit in Virginia because she purchased a policy from Genworth, a Virginia company, who contracted with PBI. This runs headlong into black-letter law. See Burger King Corp. v. Rudzewicz, 471 U.S. 462, 478 (1985) ("If the question is whether an individual's contract with an out-of-state party alone can automatically establish sufficient minimum contacts in the other party's home forum, . . . the answer clearly is that it cannot.").

Finally, Plaintiffs' only arguments for personal jurisdiction over Cruciata's claims brought in Massachusetts are (i) that Maximus entered an agreement with Progress, a Massachusetts-based company, and (ii) that Maximus has a business registration and a retained agent in the state. [Maximus Opp. at 26]. As to the first basis, it fails on the same basis as the arguments that PBI is subject to personal jurisdiction in Virginia, Washington, New York, or Illinois. See supra; see also Burger King, 471 U.S. at 478. As to the second, cases in this district have made clear that an out-of-state defendant cannot be said to be "at home" in Massachusetts, as is necessary to establish general personal jurisdiction, merely because they designate an agent

within the state. Licht v. Binance Holdings Ltd., No. 24-cv-10447, 2025 WL 625303, at *29 (D. Mass. Feb. 5, 2025).

At oral argument, the parties agreed that should the Court find personal jurisdiction lacking, it should designate an alternate venue and order the cases transferred pursuant to 28 U.S.C. § 1406(a). The cases brought by Camille and Eugene Burgan, Cruciata, and Hernandez are deemed transferred to the Eastern District of Virginia, where Maximus and Genworth are each headquartered and subject to general jurisdiction. Soto's case against PBI is deemed transferred to Minnesota, where PBI is subject to general jurisdiction. Phelan's case against TIAA is deemed transferred to New York, where TIAA is subject to general jurisdiction.

b. Common Law Claims

i. Choice of Law

Federal courts sitting in diversity apply the choice-of-law rules of the forum state to determine which state's law determines liability on common law claims. Cheng v. Neumann, 106 F.4th 19, 25 (1st Cir. 2024) ("[F]ederal courts sitting in diversity apply the substantive law of the forum state, . . . including its conflict of laws rules." (quoting Smith v. Prudential Ins. Co. of Am., 88 F.4th 40, 49 (1st Cir. 2023))). Due "to the complexities of MDL litigation," however, transferee courts in multidistrict litigation usually apply the conflict-of-law rules of the transferor court, rather than the MDL forum, to determine what law applies to common-law claims. In re Volkswagen & Audi Warranty Extension Litig., 692 F.3d 4, 14, 17–18 (1st Cir. 2012) (collecting cases). But see id. at 17 n.16 (noting that the First Circuit assumed without deciding that the transferor court's law would determine conflict of law questions). "This approach is consistent with the Supreme Court's holding that 'where a case is transferred pursuant to 28 U.S.C. § 1404(a), [a court] must apply the choice-of-law rules of the State from which the case was

transferred.'" Id. at 18 (alteration in original) (quoting Piper Aircraft Co. v. Reyno, 454 U.S. 235, 243 n.8 (1981)).

The parties largely incorporate Progress's briefing of the choice-of-law issues or otherwise reiterate the positions taken therein.[4] As such, the Court will apply the choice of law principles set forth in MDL Order No. 22. See [MDL Order No. 22 at 7–20].

In summary, the following law applies to each Defendant as to each Plaintiff:

- PBI
  - Minnesota (Jose Soto)
- Milliman Solutions, LLC; Milliman Inc.
  - Washington (Jose Soto)
- MEMBERS Life Insurance Co.
  - Wisconsin (Jose Soto)
- TIAA
  - New York (Margaret Phelan, Katharine Uhrich, Steven Teppler, Patricia Marshall)
- Genworth
  - Virginia (Camille Burgan, Eugene Burgan)
  - Texas (Tricia Hernandez)
  - New York (Gilbert Hale, Lynda Hale)
  - Florida (Patrice Hauser, Keith Bailey)
  - California (Brinitha Harris, Rita Pasquarelli)
- Welltok, Inc.
  - Rhode Island (Sherrie Rodda)
- Sutter Health
  - California (Denise Meyer, Amanda Copans)

[4] One notable variation is Delta Dental's contention that its status as an insurer compels application of the plaintiffs' home-state laws, not that of California, citing Clemco Indus. v. Commercial Ins. Co., 665 F. Supp. 3d 816, 818 (N.D. Cal. 1987). See [Delta Dental Mem. at 14–15]. The Court disagrees. In the first place, those cases involved a comparative impairment analysis—which Delta Dental's briefing fails to address. See id.; see also In re Hyundai & Kia Fuel Econ. Litig., 926 F.3d 539, 562 (9th Cir. 2019) (holding that if a party "fail[s] to meet their burden at any step in the analysis, the district court may properly find California law applicable without proceeding to the rest of the analysis"). Second, and more importantly, the conflicts analysis was tailored to the consumer protection interests at stake in a dispute concerning the "interpretation of insurance contracts." Clemco, 665 F. Supp. 3d at 818. Here, by contrast, the insurance-specific issues are relatively tangential; we are merely dealing with claims that happen to arise from the handling of data that was provided in connection with an insurer-insured relationship. The Court declines to alter its previous decision to apply California law to the California-filed claim on the ground raised by Delta Dental.

- OSF Healthcare System
  - Illinois (Chris Rehm)
- Corewell Health
  - Michigan (Tamara Williams, Jeff Weaver)
- Virginia Mason Franciscan Health
  - Washington (Megan McClendon)
- CHI Health - NE
  - Nebraska (Laquesha George)
- Delta Dental
  - California (Ricardo Moralez, Manual Mendoza, Terrill Mendler, Michelle Gonsalves, Marvin Dovberg, Deanna Duarte, Taneisha Robertson, Doris Cadet, Margaret Kavanagh, Karen Boginski, John Meeks, Yvette Tillman, Hannah Polikowsky)
  - Illinois (Diamond Roberts)
- Maximus Defendants
  - California (Shellie McCaskell)
  - Texas (Jvanne Rhodes, Aldreamer Smith)
  - New York (Barbara Cruciata)
  - Pennsylvania (Victor Diluigi)
  - Illinois (Rob Plotke)
  - Florida (Aunali Khaku, Gregory Bloch)
  - Ohio (Elaine McCoy)
  - Indiana (Alexys Taylor)
  - North Carolina (Ben Dieck)

ii. Negligence

All Defendants face allegations of common-law negligence, and the parties dispute whether Plaintiffs have adequately alleged the familiar elements of a negligence claim: breach of a duty, causing the plaintiff's damages. The Court addresses each element in turn.

1. Duty and Breach

The negligence claims at issue in this case center on allegations that both the direct-user and VCE Defendants owed, and breached, duties to protect Plaintiffs' personal information. Defendants, as they made clear during oral argument before this Court, do not dispute that they owe some duty to protect Plaintiffs' information. They maintain, however, that Plaintiffs' conception of Defendants' duties reaches too far.

Plaintiffs' theory of duty as to the non-Progress Bellwether Defendants centers on their failure to ensure that industry-standard cybersecurity procedures were in place. Plaintiffs allege that those procedures should have included:

- security audits of the MOVEit Transfer software, e.g., [CAC ¶ 1977];
- auditing of Progress's cybersecurity practices, e.g., [id. ¶ 1978];
- restricting the IP addresses that could access the MOVEit Transfer interface ("whitelisting"), e.g., [id. ¶ 1979];
- limiting the file types that could be uploaded to MOVEit Transfer, e.g., [id. ¶¶ 1980–81];
- implementing logging and monitoring programs that might have detected CL0P's intrusion before it executed harmful code, e.g., [id. ¶¶ 1982–87].

The duty manifests differently between direct-user Defendants and VCE Defendants. In Plaintiffs' telling, the direct-user Defendants (PBI, Delta Dental, Maximus, and Welltok), as the holders of software licenses from Progress, and therefore as the entities who had control over the MOVEit Transfer software installed on their servers, had a duty to implement these procedures on their computer systems. See, e.g., [CAC ¶ 1975]. The VCE Defendants (Genworth, TIAA, Corewell, etc.), who contracted with the direct users and shared Plaintiffs' data through the MOVEit software, had a duty to ensure that the direct users had implemented these or other comparable safeguards to protect Plaintiffs' data before sharing it. See, e.g., [CAC ¶ 2014]. Broadly speaking, Plaintiffs contend that the VCE Defendants had a duty to vet the direct users' security practices before contracting with them and a duty thereafter to audit the direct users periodically.

a. Direct user duty and breach

As to some of the cybersecurity measures that Plaintiffs list in the complaint, Defendants dispute whether they had any duty to implement such steps. They argue, for example, that they owed no duty to audit the MOVEit software. See, e.g., [PBI Mem. at 37–38]. As to other security measures, however, there does not appear to be any dispute that Defendants' duty of care

encompassed an obligation to appropriately configure the MOVEit application, to restrict the IP addresses that could access the MOVEit interface, or to restrict the file types that could be uploaded. These steps, Plaintiffs plausibly allege, are industry standards that a reasonable entity in the direct users' position would have implemented, particularly to the extent Progress itself recommended that they do so.

Accepting that they owed duties of care in this regard, the direct users contend that Plaintiffs have not plausibly alleged that they breached any such duties. The direct users contend that Plaintiffs' theory of breach depends on an implausible post hoc propter hoc inference that merely because a data breach occurred, Defendants must not have implemented whitelisting or file-type restrictions. See, e.g., [Welltok Mem. at 36].

Contrary to the direct users' arguments, the breach-of-duty allegations in the CAC are not just conclusory assertions. See, e.g., [ECF No. 1360 at 31–32]. Rather, the CAC alleges technical details of the CL0P attack based on forensic reports from the private sector and government actors, [CAC ¶¶ 1074–124], and alleges that specifically identified industry-standard precautions would have prevented CL0P from accessing Plaintiffs' data, [id. ¶¶ 1977–87]. For example, the allegations against PBI describe how, "[h]ad PBI limited the specific types of files that could be uploaded" via MOVEit Transfer, it "could . . . have prevented the Data Breach" because CL0P's attack depended on uploading a web shell that "masqueraded as a legitimate file and allowed the threat actor to execute commands, download files, extract system settings, and create/insert/delete users." [CAC ¶ 1980]. The CAC alleges that restricting the uploading of such files to "whitelisted IP addresses" would have prevented the web shell file that CL0P used to hijack the secure data environment. [Id. ¶ 1981]. Given these particularized allegations, the

CAC states a "plausible" claim that the direct users breached their duty to take reasonable measures to safeguard Plaintiffs' data.

b. VCE duties

The VCEs do not dispute that when a defendant collects a plaintiff's PII, the defendant takes on "a duty to protect [t]he [p]laintiffs from foreseeable harm by taking reasonable precautions to safeguard" their PII. In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig. (AMCA), No. 19-mc-02904, 2021 WL 5937742, at *14 (D.N.J. Dec. 16, 2021). They do not even seriously contest that their duty to safeguard Plaintiffs' PII included an obligation to vet the direct users, [PBI Mem. at 30–31], acknowledging in their motion that negligence law generally imposes a duty of "reasonable care to employ a competent and careful contractor," Restatement (Second) of Torts § 411 (1965). The VCEs insist, however, that such a duty does not require "an elaborate investigation as to the competence of a contractor," particularly a contractor with a "good reputation." Id. § 411 cmt. c. Though the VCEs do not draw a line delineating what their duty to vet the direct users entailed, they insist that, for example, PBI's public statements that it "follows the . . . NIST Cybersecurity Framework" should have discharged any duty to inquire on the part of TIAA or the other PBI VCEs. [PBI Mem. at 32].

The case law does not support the VCE's suggestion that their duty of care is automatically discharged by hiring a contractor. A defendant does not avoid its duty simply by stashing data in a "database that is in the possession of a third-party vendor" or independent contractor. AMCA, 2021 WL 5937742, at *15. "[T]he reasonably foreseeable risk of danger of a data breach incident" means that, in the context of corporate cybersecurity, even though common law principles do not require a defendant to "oversee all of [an independent contractor]'s

operations," the mere interposition of a reputable independent contractor "does not absolve Defendants of their duty to take reasonable care by, for example, reasonably ensuring that the [direct users] they contracted with had adequate data security." Id. at *14–15.

Moreover, the Court is skeptical of the VCEs' contention that, as a matter of law, their duty only could be fulfilled by obtaining a blanket assurance from vendors that, as in the example of PBI, they comply with the NIST Framework. The reasonableness of their conduct, after all, depends on the circumstances. To be sure, the PBI VCEs point to an array of circumstances they say inform the relevant standard of care. For example, they advert to PBI's good reputation, the fact that PBI's death-matching services are required by law, and that nearly the entire life-insurance industry contracts and shares policyholder data with PBI for that purpose. [PBI Mem. at 31–32]. As a factual matter, such arguments may ultimately prove persuasive—but this is not an issue that can be resolved at the pleading stage. It remains to be developed in discovery whether PBI's status as the only game in town for a service for legally-mandated data-matching services made it a likely and foreseeable target for a data breach, such that a reasonable inquiry into its cybersecurity competence would require more than their say so. Plaintiffs' allegations suffice, if barely, to support a plausible inference that a reasonable company under the circumstances would have confirmed that the direct user's assurances were backed up by reality.

2. Causation and Damages

Although causation typically precedes damages in the negligence analysis, the Court nevertheless turns to damages first, as causation of a cognizable harm turns on whether a cognizable harm exists.

Defendants argue that Plaintiffs' allegations of risk of future harm, lost time, increased spam, and lost value of PII are not compensable and that Plaintiffs have not alleged actual non-compensated monetary loss. [PBI Mem. at 41–42; Delta Dental. Mem. at 58–59; Maximus Mem. at 34]. As we have established in MDL Order No. 22, damages have been adequately pleaded by Plaintiffs. First, several Plaintiffs allege that they have already experienced identity theft or other forms of misuse, which are obviously cognizable. See [CAC ¶¶ 88 (Diluigi); 143 (McCoy); 161 (Plotke); 178 (Rhodes); 213 (Taylor); 231 (Williams); 294 (Meyers); 315 (Rehm); 334 (Rodda); 356 (George); 688 (Camille Burgan) 706 (Eugene Burgan); 723 (Gilbert Hale); 740 (Lynda Hale); Harris (757); Hauser (774); 792 (Hernandez); 809 (Pasquarelli); 841 (Checchia); 859 (Marshall); 876 (Phelan); 893 (Teppler); 910 (Uhrich)]; see, e.g., Weekes v. Cohen Cleary P.C., 723 F. Supp. 3d 97, 103 (D. Mass. 2024); In re Accellion, Inc. Data Breach Litig., 713 F. Supp. 3d 623, 637 (N.D. Cal. 2024); Bohnak v. Marsh & McLennan Cos., 79 F.4th 276, 289–90 (2d Cir. 2023). This, at the very least, applies to all claims against TIAA, Genworth, Welltok Inc., OSF, Corewell, and CHI Health - NE, and most of the claims against Maximus. Second, all Plaintiffs allege an increased risk of future misuse, which, in light of the allegations of actual misuse, are not unduly speculative. Third, many Plaintiffs allege that they have spent time, money, or both addressing the fallout from the Data Breach. Such allegations are non-speculative in light of the Plaintiffs' properly pled allegations of a risk of future harm. See, e.g., Bohnak, 79 F.4th at 290; Webb v. Injured, No. 22-cv-10797, 2023WL 5938606, at *2 (D. Mass Sep. 12, 2023). Fourth, at this stage, many Plaintiffs have adequately pleaded specific enough manifestations of their emotional distress to survive a motion to dismiss.

Thus, the Court turns to the adequacy of the CAC's allegations regarding the cause of the damages in question. Defendants argue that there is no causation because this was a "zero-day"

event. Defendants also contend that the alleged harms do not really map to the data that was allegedly stolen—rebutting any inference that the harms were caused by the CL0P exploit. [PBI Mem. at 41; Welltok Mem. at 38; Delta Dental Mem. at 59; Maximus Mem. at 34]. Plaintiffs respond that causation is a question of fact ordinarily decided by the jury, and that the arguments here do not overcome that presumption. See, e.g., [PBI Opp. at 39–40]. They argue that the "zero-day" argument fails because both the direct users and the VCEs could have taken further preventative steps to secure the data, even if they did not learn of this particular security vulnerability until the attack was underway. [Id.]. They also argue that the "data mismatch" theory is not ripe for decision on the pleadings; that it is premature to decide such a factual dispute at this time. [Id. at 23].

The "zero-day" argument is unpersuasive. Even though Defendants did not know about this particular vulnerability prior to the attack, if they failed to take proper precautionary measures or failed to adequately vet their vendors, that is sufficient for proximate causation.

The data mismatch theory may ultimately prove determinative—it suggests a facially plausible argument that events other than the CL0P may have caused some of the identified harms. But the Court agrees with Plaintiffs that this is ultimately a factual issue, requiring a more developed record. For present purposes, the CAC adequately alleges that Plaintiffs suffered damages stemming from the CL0P data breach.

3. Economic Loss Doctrine

All Bellwether Defendants contend that the economic loss doctrine should bar Plaintiffs' negligence claims arising under California, Illinois, Pennsylvania, Texas, Ohio, and Indiana law. See [PBI Mem. at 27–28; Delta Dental Mem. at 57–58; Welltok Mem. at 39; Maximus Mem. at 44–46]. The economic loss doctrine is a complex and esoteric common law principle of relatively recent vintage, which purports to limit remedies for tort claims that "seek[]to recover

for a commercial loss rather than damage to person, property, or reputation." Miller v. U.S. Steel Corp., 902 F.2d 573, 574 (7th Cir. 1990). Despite the doctrine's complexity, the parties spill very little ink on the issue; indeed, the considerable variations in how particular states apply the doctrine are addressed only in string citations and footnotes. See, e.g., [PBI Mem. at 28 n.3; Maximus Mem. at 44–46]. As in the MDL Order No. 22, in light of the foregoing, the Court declines to dismiss Plaintiffs' negligence claims on economic loss grounds, but will permit Defendants to brief the issue anew at a later stage.

The Court therefore **DENIES** the motion to dismiss as to Count I for all Defendants.

iii. Negligence Per Se

Plaintiffs allege that the PBI Bellwether Defendants, Delta Dental, and the Welltok Bellwether Defendants are liable for negligence per se because they allegedly violated statutes or regulations that establish duties of care, in particular, the Federal Trade Commission Act ("FTC Act"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the Health Insurance Portability and Accountability Act ("HIPAA"), the HIPAA Privacy Rule and Security Rule, and the Gramm-Leacy-Bliley Act ("GBLA"), as well as "similar state statutes." [CAC ¶¶ 2096, 2098, 2611].

Defendants collectively urge dismissal on several grounds: (1) several of the relevant jurisdictions (California, Illinois, Michigan, Nebraska, New York, Pennsylvania, Tennessee, Texas, and Washington) do not recognize negligence per se as a standalone cause of action, [Delta Dental Mem. at 59–60; Welltok Mem. at 40]; (2) several additional jurisdictions (Florida, North Carolina, South Carolina, and Tennessee) do not recognize negligence per se unless the underlying statute confers a private right of action (which the statutes at issue, the FTC Act and HIPAA, indisputably do not), [Delta Dental Mem. at 60, PBI Mem. at 44]; (3) even in other jurisdictions, the FTCA and GBLA do not support negligence per se claims, [PBI Mem. at 43 &

n.16]; and (4) plaintiffs have not shown that the violation of any statute was a cause of compensable damages, [Delta Dental Mem. at 61].

Plaintiffs provide no response on the first point. See, e.g., [Delta Dental Opp. at 41]. That resolves Count II against Delta Dental, for which the motion to dismiss is **GRANTED**, as well as Count II pertaining to the relevant Plaintiffs against the PBI Bellwether Defendants and Welltok Defendants . As to the second point, Plaintiffs argue generally that federal statutes without a private right of action can give rise to a negligence per se claim, but Plaintiffs do not address the state laws specifically referenced by Defendants. See, e.g., [id. at 41]. Given that liability here would ultimately rest upon state common law, the motion to dismiss is **GRANTED** with respect to Florida, North Carolina, South Carolina, and Tennessee.

That leaves Rhode Island (Welltok, Inc.), Virginia (Genworth), Minnesota (PBI), and Wisconsin (MEMBERS Life Insurance Co.).

PBI argues that the remaining claims must be dismissed because the CAC fails to allege violations of section 5 of the FTC Act and the GBLA. [PBI Mem. at 44]. PBI's argument largely rises and falls with its negligence argument. [Id. at 43 ("These claims both fail because the underlying negligence claims do."); id. at 44 ("Regardless, Plaintiffs' allegations that the PBI Contracting Defendants violated Section 5 and the GLBA fail for reasons similar to those pertinent to Plaintiffs' inability to adequately allege breach for their negligence claim."); id. at 24 ("Plaintiffs' allegations suffer from the same lack of factual support that plagues their negligence allegations.")]. Because the Court disagrees with PBI on the negligence claims, it necessarily disagrees with PBI for the remaining negligence per se claims, and the motion to dismiss is therefore **DENIED** as to the claims under Virginia, Minnesota, and Wisconsin law. And as

Welltok did not address whether these theories of negligence per se would be available under Rhode Island law, the motion is **DENIED** on that front as well.

iv. Invasion of Privacy: Intrusion Upon Seclusion and Public Disclosure of Private Facts

Plaintiffs allege that the PBI Bellwether Defendants, Delta Dental, and Maximus are liable for invasion of privacy on both intrusion-upon-seclusion and public-disclosure theories. [CAC ¶¶ 2111–30, 2691–712, 3090–3111]. As a threshold matter, there is no common-law right of action for invasion of privacy in New York. Waldron v. Ball Corp., 619 N.Y.S.2d 841, 844 (App. Div. 1994). This disposes of various claims against TIAA.[5]

All of Plaintiffs' public-disclosure claims fail to allege key elements. To state a claim for public disclosure of private facts, a plaintiff must allege "(1) public disclosure, (2) of a private fact, (3) which would be offensive and objectionable to the reasonable person, and (4) which is not of legitimate public concern." Taus v. Loftus, 151 P.3d 1185, 1207 (Cal. 2007); see also Restatement (Second) of Torts § 652D (1977) ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."). The first prong "presume[s] a publication made by the defendant," Caraccioli v. Facebook, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016) (citing Taus, 151 P.3d at 1185). Defendants here are correct in pointing out that the CAC does not allege that Defendants ever made a public disclosure of Plaintiffs' data (only CL0P did). [Delta Dental

[5] The parties do not make jurisdiction-specific arguments with respect to the seclusion/public-disclosure claims, with just one relevant exception: the claims against TIAA, which are governed by New York law based on the conflict of law rules of New York, Minnesota, and Illinois, all fail because New York does not recognize a "common-law right of action for invasion of privacy." Waldron, 619 N.Y.S.2d, at 844. Plaintiffs abandon their North Carolina and New York privacy tort claims for the same reason. [Maximus Opp. at 57 n.49].

Mem. at 44; PBI Mem. at 46; Maximus Mem. at 49]. Plaintiffs do not dispute Defendants' characterization of the factual allegations of the CAC, but contend that "Plaintiffs can satisfy this requirement through allegations that the defendant affirmatively shared information or performed some act that made the plaintiff's information known," [Maximus Opp. at 59 (cleaned up)]. The problem with this argument—as Delta Dental, for example, notes in response—is that the case Plaintiffs rely on addresses a claim for invasion of privacy under the California Constitution, which does not require public disclosure as an element. [Delta Dental Reply at 21–22]; see In re Ambry Genetics Data Breach Litigation, 567 F. Supp. 3d 1130, 1143 (quoting In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 601 (9th Cir. 2020)) (reciting the elements of an invasion of privacy claim under the California Constitution).

The Court agrees with Defendants that this case is akin to the unsuccessful public-disclosure claim against Progress and that the case law rejects such claims when premised on public disclosure by third party hackers (rather than the defendant). See, e.g., Liberi v. Taitz, No. SACV 11-0485 AG, 2011 WL 13315688, at *3 (C.D. Cal. Sept. 12, 2011) ("Plaintiffs do not allege that Oracle publicly disclosed any of their private information. Instead, Plaintiffs allege that Oracle failed to address vulnerabilities in its architecture, thereby leading to the disclosure of their private information."); Caraccioli, 167 F. Supp. 3d at 1063; McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810, 820 (E.D. Ky. 2019) (holding that in jurisdictions following the restatement "[c]ases addressing similar data breaches have concluded that unauthorized disclosure of personal information does not constitute publication"); Webster v. Bradford-Scott Data, LLC,

No. 24-cv-00117, 2025 WL 560917, at *12 (N.D. Ind. Feb. 20, 2025) ("This Court has been critical of extending Indiana's public-disclosure tort to data breach cases such as this.").[6]

Plaintiffs do not dispute that "a hacker's access to PII does not constitute the defendant's disclosure to the public," but argue as a fallback that the publicity element can be "satisfied by disclosure to a limited number of people if . . . the disclosure [is] as devastating as disclosure to the public at large." [PBI Opp. at 51 (alterations in original) (quoting Karraker v. Rent-A-Ctr., Inc., 411 F.3d 831, 838 (7th Cir. 2005))]. What Plaintiffs omit from Karraker through alterations, however, is key: the publicity element can be "satisfied by disclosure to a limited number of people if those people have a special relationship with the plaintiff that makes the disclosure as devastating as disclosure to the public at large." 411 F.3d at 838 (emphasis added). Plaintiffs make no argument, nor do they allude to any allegation in the CAC, to support their contention that the allegations here would somehow satisfy the "special-relationship" requirement

The analysis is similar for claims for intrusion upon seclusion. A plaintiff must plead two elements: "[f]irst, the defendant must [have] intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy." Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1072 (Cal. 2009). "Second, the intrusion must [have] occur[ed] in a manner highly offensive to a reasonable person." Id.; accord Accellion, 713 F. Supp. 3d at 646 (N.D. Cal. 2024) (same); see also Restatement (Second) of Torts § 652B (1977) ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

[6] Although many of the citations in this section are to California law, no party alleges a material conflict on this claim.

Defendants insist that, in light of the intentional-intrusion requirement, common law does not recognize that an alleged "failure to take adequate measures to protect against the intentional intrusion of a third party satisfies the first element of a claim for intrusion on seclusion." Damner v. Facebook Inc., No. 20-cv-05177, 2020 WL 7862706, at *6 (N.D. Cal. Dec. 31, 2020); [Delta Dental Mem. at 43]; see also Mirfendereski v. Rakestraw, No. 10-CV-306, 2011 WL 3584325, at *9 (S.D. Ohio Aug. 15, 2011) (finding negligence insufficient for invasion of privacy). Thus, they argue, Plaintiffs' allegations do not describe any "intentional act to intrude upon" their private affairs, [Delta Dental Mem. at 43], but allege only that they "fail[ed] to keep [their] Private Information safe," [CAC ¶ 2704]; see also [PBI Mem. at 47; Maximus Mem. at 47]. In response, Plaintiffs assert generally that they have "pled that [Delta Dental] intentionally failed to adequately safeguard their data," [Delta Dental Opp. at 50 (citing CAC ¶¶ 2701–12)]. But this is mere wordplay. Adding the adverb "intentionally" does not disguise the glaring absence from the CAC of any non-conclusory factual allegation that any Defendant took intentional action to intrude upon a protected interest.

Along the same lines, as to the intrusion-upon-seclusion claims against the PBI Bellwether Defendants, Plaintiffs say that the CAC establishes that those Defendants "knew their security practices were inadequate to safeguard Plaintiffs' PII and would likely result in a breach that would harm Plaintiffs." [PBI Opp. at 50]. Yet even an allegation that PBI knew better than to configure its security the way it did, or "intentionally fail[ed] to keep Plaintiffs' PII safe," still falls short of a plausible allegation that PBI intentionally intruded upon Plaintiffs' privacy. Andersen v. Oak View Grp., LLC, No. 24-cv-00719, 2024 WL 5426654, at *5 (C.D. Cal. Nov. 22, 2024).

The California Constitutional right to privacy claim against Welltok fails for similar reasons. Plaintiffs Copans and Meyer allege only that "Welltok's and Sutter's negligent data security practices resulted in the compromise and exfiltration of Plaintiffs' Private Information, including their health insurance information, provider names, treatment cost information, and treatment information or diagnoses." [Welltok Opp. at 59 (emphasis added)].

The only argument that Plaintiffs add to the mix with respect to Maximus is an assertion that in California and Illinois, the public disclosure of medical information receives heightened protection relative to the other information at issue in a claim for tort recovery. [Maximus Opp. at 58 & n.50 (first citing Stasi v. Inmediata Health Grp. Corp., 501 F. Supp. 3d 898, 910 (S.D. Cal. 2020), and then citing Di Benedetto v. J. Lais, No. F060165, 2011 WL 1798074, at *5 (Cal. Ct. App. May 11, 2011))]. The cases they cite, however, do not support their assertion. In Stasi, the court merely acknowledged, in the course of analyzing Article III standing, that the "harm that results from 'posting' medical information on the internet has a close relationship to harm that has traditionally been regarded as providing a basis for a lawsuit, especially the public disclosure of private facts." 501 F. Supp. 3d at 910. Di Benedetto similarly stated only that "an unauthorized disclosure of private medical information can constitute a tortious and actionable public disclosure of private facts," 2011 WL 1798074, at *5, but did not purport to alter the elements of such a claim when the disclosure involved medical information.

Consequently, the motion to dismiss the common law privacy claims (Claims 3 and 4 against PBI, 5 and 6 against Maximus, and 7 and 8 against Delta Dental) are **GRANTED**. Because Plaintiffs concede that the common-law intrusion claim and the California Constitution right-to-privacy claim rise and fall together, see [Delta Dental Opp. at 34], the motions to dismiss

Count 16 against Delta Dental and Count 12 against Maximus are also **GRANTED**. The motion to dismiss Count 12 against Welltok is also **GRANTED**.

v. Breach of Implied Contract

1. Delta Dental (Count 3)

Plaintiffs allege that Delta Dental, the Welltok VCEs, TIAA, MLIC, Milliman, and Genworth are liable for breach of implied contract, and in the case of Delta Dental and the Welltok VCEs, Plaintiffs point to Defendants Privacy Policies as evidence of the terms of such implied contracts. [CAC ¶¶ 2131–46, 2625–49, 3556–74]. Plaintiffs argue that they were required to provide their PII to the relevant Defendants, which created an implied promise to safeguard the data. For example, as against Delta Dental, Plaintiffs argue that "[b]y agreeing to safeguard Plaintiffs' sensitive Private Information in exchange for their business, [Delta Dental] and Plaintiffs entered into implied contracts." [Delta Dental Opp. at 28–29]; see also [PBI Opp. at 46; Welltok Opp. at 40–41].

All Defendants dispute the existence of an implied contract. According to Delta Dental and the Welltok VCEs, the Privacy Policies did not represent a promise to safeguard Plaintiffs' data in exchange for their business, but rather, described the manner of their compliance with legal and regulatory obligations that exist independent of any particular consumer relationship. [Delta Dental Mem. at 49–50; Welltok Mem. at 47]. All three groups of Defendants also argue that Plaintiffs have not pleaded facts supporting mutual assent to privacy or cybersecurity terms because Plaintiffs do not allege factual circumstances supporting the inference that there was a meeting of the minds about cybersecurity. [Delta Dental Mem. at 50; Welltok Mem. at 45; PBI Mem. at 50]. TIAA, Genworth, and MLIC argue that the existence of a written contract precludes the existence of an implied contract, [PBI Mem. at 49], and Milliman argues that Plaintiff Soto did not even know Milliman existed much less have any direct dealings with them,

[PBI Mem. at 50]. The PBI VCEs also argue that, under certain state law, pecuniary loss is required for a breach of implied contract claim. [PBI Mem. at 52].

Under common law, "[a]n implied-in-fact contract requires proof of the same elements necessary to evidence an express contract: mutual assent or offer and acceptance, consideration, legal capacity and lawful subject matter." Landon v. TSC Acquisition Corp., No. 23-cv-01377 2024 WL 5317240, at *9 (C.D. Cal. Nov. 1, 2024) (quoting Corona v. Sony Pictures Ent., Inc., No. 14-CV-09600, 2015 WL 3916744, at *6 (C.D. Cal. June 15, 2015) (citation omitted)).

The Court concludes that Plaintiffs' implied-contract theory against Delta Dental and the Welltok VCEs fails for lack of consideration and, thus, declines to reach those Defendants' other arguments for dismissal. It is black letter law, in California as in other jurisdictions, that a "statutory or legal obligation to perform an act may not constitute consideration for a contract." O'Byrne v. Santa Monica-UCLA Med. Ctr., 94 Cal. App. 4th 797, 808 (Cal. Ct. App. 2001) (citing Cal. Code Regs. tit. 22, §§ 70701, 70703). Thus, although an implied contract can exist where a Privacy Policy "promises that reasonable security measures will be taken," and the plaintiff "alleges [that the defendant] did not take those precautions," Landon, 2024 WL 5317240, at *10, a promise to apply reasonable cybersecurity measures only "constitutes valid consideration" to the extent "the promise is a voluntary duty not imposed by law," Walters v. Kimpton Hotel & Rest. Grp., LLC, No. 16-cv-05387, 2017 WL 1398660, at *2 (N.D. Cal. April 13, 2017).

Delta Dental contends that, as a matter of law, the CAC fails to allege an exchange of consideration, given Plaintiffs' allegation that Delta Dental's implied promise to safeguard their information was, at most, coextensive with its obligations under HIPAA and other existing legal obligations. [Delta Dental Mem. at 49]. The CAC does indeed describe the factual content of

Delta Dental's alleged promises in those terms. Specifically, Plaintiffs refer to the Delta Dental Plans Association's Privacy Policy,[7] which states that the company engages in data practices "consistent with the terms of applicable HIPAA business associate agreements." [CAC ¶ 2434]. Another privacy statement promises to "employ reasonable safeguards designed to promote the security of our systems." [Id. ¶ 2435]; accord [id. ¶ 2417].

The Court agrees with Delta Dental that in the context of HIPAA-covered entities or business associates, a promise to provide "reasonable safeguards," without more, does not constitute a commitment beyond the entity's existing regulatory obligations under the HIPAA Security Rule. See, e.g., 45 C.F.R. § 164.306(b)(1) (allowing covered entities and business associates to "use any security measures that allow [them] to reasonably and appropriately implement the standards and implementation specifications as specified in [the rule]"). This feature of the dispute involving Delta Dental sets it apart from the cases that Plaintiffs cite which did not involve HIPAA-covered entities. E.g., Walters, 2017 WL 1398660, at *2 (denying hospitality company's motion to dismiss breach of implied contract claim where the plaintiff "plausibly alleged the existence of an implied contract arising from [defendant's] privacy policy, which states that [defendant] is 'committed' to safeguarding customer privacy and personal information").[8] The same logic applies for the Welltok VCEs: a hospital's promise to keep

[7] Although Plaintiffs stipulated to the dismissal of the Delta Dental Plans Association as a defendant in the bellwether cases, both parties continue to premise their contract arguments on its Privacy Policies. The Court thus assumes without deciding that the Delta Dental Plans Association's statements can be imputed to the Delta Dental Defendants that remain in this litigation.

[8] Plaintiffs' other case law to the effect that "mandatory receipt" of their data as part of Delta Dental's medical insurance offering should "impl[y] the recipient's assent to protect the PII sufficiently," Medoff v. Minka Lighting, LLC, No. 22-cv-08885, 2023 WL 4291973, at *10 (C.D. Cal. May 8, 2023), is distinguishable for similar reasons.

patient information confidential does not constitute consideration for an alleged contract due to the hospital's preexisting duty to protect that information. See, e.g., Alar v. Mercy Mem'l Hosp., 529 N.W.2d 318, 322 (Mich. Ct. App. 1995).

The motion to dismiss Count 3 against Delta Dental and Count 4 against Welltok is **GRANTED**. Because under California law, there can be no implied covenant of good faith and fair dealing absent "some specific contractual obligation," Avidity Partners, LLC v. State, 165 Cal. Rptr. 3d 299, 320 (Cal. Ct. App. 2013), the motion to dismiss Count 4 against Delta Dental, breach of implied covenant of good faith and fair dealing, is also **GRANTED**.

That leaves the claims against the PBI Bellwether Defendants. First, the Court addresses Plaintiff Soto's claims against the Milliman Defendants. The Milliman Defendants argue that there could be no meeting of the minds with Plaintiff Soto because he was a customer of MLIC, which separately contracted with Milliman, and therefore neither party knew of the other's existence. [PBI Mem. at 71–72]. Soto's rejoinder is that this raises a premature factual dispute. [PBI Opp. at 48]. The Court disagrees: the basis of Plaintiffs' argument is that handing over data to a company creates an implicit agreement to protect that data, and there is no allegation that Soto knowingly gave Milliman his information. In re Arthur J. Gallagher Data Breach Litig., 631 F. Supp. 3d 573, 591 (N.D. Ill. 2022) ("The remaining Plaintiffs had no direct dealings with Defendants and were unaware of Defendants' existence until they received notice from them of the Data Breach. They thus could not have reached any implied understanding with Defendants.").

TIAA and Genworth's other arguments, however, are less persuasive. First, the existence of a written contract is not dispositive as to the existence of implied contractual terms. See Attias v. CareFirst, Inc., No. 15-CV-882, 2023 WL 5952052, at *5 (D.D.C. Sept. 13, 2023). Moreover,

for similar reasons as discussed supra, Plaintiffs have adequately plead damages in the relevant states; indeed, at least one Plaintiff claims actual identity theft under all of the states' laws governing the claims. With regard to assent, in arguing that the mere act of providing data to a party does not necessarily obligate the recipient to safeguard such data, Plaintiff relies on cases that address circumstances very different from the matter at law. For example, in Longenecker-Wells v. Benecard Servs. Inc, the Court held that there was no implied contract because there were no "company-specific documents or policies from which one could infer an implied contractual duty to protect Plaintiffs' information." 658 F. App'x 659, 663 (3d Cir. 2016). Here, the CAC alleges that Defendants' policies can support just such a conclusion, [CAC ¶ 2134], and even if these were internal policies, [PBI Reply at 24], they may support an inference regarding Defendants' course of conduct. PBI Defendants' motion to dismiss Count 5 is therefore **DENIED**.

vi. Breach of Confidence

Plaintiffs raise a breach of confidence claim against Delta Dental.[9] [CAC ¶¶ 2659–74]. To state a claim for breach of confidence under California law "a plaintiff must allege that '(1) the plaintiff conveyed "confidential and novel information" to the defendant; (2) the defendant had knowledge that the information was being disclosed in confidence; (3) there was an understanding between the defendant and the plaintiff that the confidence be maintained; and (4) there was a disclosure or use in violation of the understanding.'" Ambry, 567 F. Supp. 3d at

[9] Under California law, a breach of confidence tort "is based upon the concept of an implied obligation or contract between the parties that confidential information will not be disclosed." In re Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 409 (E.D. Va. 2020) (citation omitted); see also id. at 410 n.22 (finding that breach of confidence claims and claims for breach of an express contract are mutually exclusive). Although Delta Dental denies the existence of an implied contract (and the Court agrees), it does not urge dismissal of the breach of confidence claim based on the absence of an implied contract. The Court thus addresses the breach of confidence claim on the grounds raised.

1146. Delta Dental contends that the claim should be dismissed per the fourth prong, because California cases interpreting the "ordinary meaning of the word disclosure suggest[] that disclosure occurs when the [defendant] affirmatively shares medical information with another person or entity." Id. (internal quotation marks omitted) (quoting Sutter Health v. Superior Ct., 174 Cal. Rptr. 3d 653, 659 (Cal. Ct. App. 2014)). Delta Dental contends that the allegations concerning the Data Breach do not support an inference that it affirmatively shared Plaintiffs' medical information. [Delta Dental Mem. at 46–47].

Plaintiffs respond that they "need only allege 'that the defendant "affirmatively shared [] information" or performed some "act that made [the plaintiff's] information known."'" [Delta Dental Opp. at 28 (quoting Farmer v. Humana Inc., 582 F. Supp. 3d 1176, 1189 (M.D. Fla. 2022) (alternation in original) (first quoting Ambry, 567 F. Supp. 3d at 1147; and then quoting In re Brinker Data Incident Litig., No. 18-CV-686-J-32MCR, 2020 WL 691848, at *22 (M.D. Fla. Jan. 27, 2020)). They assert that allegations that Delta Dental "failed to whitelist or restrict certain file types, did not follow security recommendations, and allowed executable code to be run on their servers" satisfies California's legal standard. [Delta Dental Opp. at 28 (citing ¶¶ 2499–2500, 2522–29)].

These allegations amount to an assertion that Delta Dental's inadequate security facilitated the theft of information by third parties. In such circumstances, Plaintiff's own case law acknowledges that "a breach of confidence claim does not lie" when "a defendant's inadequate security facilitated the theft of information by third parties." Farmer, 582 F. Supp. 3d at 1189 (cleaned up and emphasis added) (quoting Brinker, 2020 WL 691848, at *22). As Delta Dental explains, the Farmer case still enforced the requirement of an affirmative disclosure (applying Florida law), and dismissed the claim before it "because there [were] no alleged facts

suggesting that [the] [d]efendant[s] disclosed [the] [plaintiff's] information to a third party." Id. (internal citation omitted). Rather, the plaintiff in that case merely "allege[d] that his PII and PHI were exposed in a data breach due to [defendants'] failure to adequately safeguard this information," which was insufficient to state a claim. Id.

Here, the Court agrees with Delta Dental that Plaintiffs' allegations, which the Court must take as true, boil down to accusations about security measures that Delta Dental should have taken and do not describe an affirmative disclosure of confidential information. Thus, there is no allegation that supports a claim for breach of confidence. Plaintiffs' citations are unpersuasive. In In re Capital One Consumer Data Sec. Breach Litig., the Eastern District of Virginia summarily concluded that the plaintiffs had stated a claim for breach of confidence without addressing the affirmative-sharing requirement. 488 F. Supp. 3d 374, 409 (E.D. Va. 2020). It did not opine one way or the other on the question now before the Court. As to Wallace v. Health Quest Systems, Inc., that case interpreted New York law, which "recognize[s] [that a duty of confidentiality] may be breached through negligent failure to safeguard confidential information." No. 20-cv-545, 2021 WL 1109727, at *13 (S.D.N.Y. Mar. 23, 2021). California applies a different standard. Ambry, 567 F. Supp. 3d at 1146–47. The motion to dismiss the breach of confidence claim against Delta Dental is **GRANTED**.

The CAC also alleges a breach of confidence claim in Count 7 against Maximus, although the Plaintiffs whose tort claims are governed by Indiana, North Carolina, and Virginia law have expressly abandoned their breach of confidence allegations. [Maximus Opp. at 58 n.51]. Maximus's motion to dismiss Count 7 is, as a threshold matter, **GRANTED** as to

Plaintiffs Taylor and Dieck.[10] The Court also agrees that there is no action for breach of confidence in Texas outside of trade secret violations,[11] a point to which Plaintiffs have offered no response, and the motion is therefore also **GRANTED** as to Plaintiffs Rhodes and Smith.

As to the claims governed by Pennsylvania, New York, Florida, and Illinois law, Maximus urges dismissal for failure to plead a "direct relationship of confidence," such as a "confidential business relationship, a statutory relationship (e.g. doctor patient), or a relationship in the trade secret context." [Maximus Mem. at 28 (citing cases)]. Plaintiffs appear to agree, recognizing that "the core of [a breach of confidence] claim 'involves the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship.'" [Maximus Opp. at 58 (emphasis omitted) (quoting Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114 (3d Cir. 2019))].

In opposing Defendant's motion to dismiss, Plaintiffs merely recite that they "allege Maximus received nonpublic information within such a confidential relationship," [Maximus Opp. at 58 (citing CAC ¶ 3115)], and point to the allegation that "Maximus has a special relationship with those whose Private Information it maintains," [CAC ¶ 3115]. This is a textbook example of a legal conclusion, as opposed to a factual allegation. Plaintiffs also cite paragraph 2935 of the Complaint, which alleges that Maximus's contact with the State of

[10] Based on the Court's personal jurisdiction analysis above, Plaintiff Cruciata's claim is governed by New York, rather than Virginia law. Consequently, there are no Maximus Plaintiffs for whom Virginia law is relevant.

[11] Maximus makes this point in its opening brief. See [Maximus Mem. at 50–51]; In re Waste Mgmt. Data Breach Litig., 21-cv-6147, 2022 WL 561734, at *3 (S.D.N.Y. Feb. 24, 2022) ("Under Texas law, breach of confidence is an element of a claim for misappropriation of trade secrets, and may not exist as a separate cause of action.") (first citing Motion Med. Tech. v. Thermotek, Inc., 875 F.3d 765, 775 (5th Cir. 2017); and then citing Hyde Corp v. Huffines, 314 S.W.2d 763, 777 (Tex. 1958)). Plaintiffs offer no response, which Maximus asserts constitutes waiver. See [Maximus Opp. at 58–59]; [Maximus Reply at 22 n.25].

Tennessee promised "strict standards of confidentiality of records" and that "information provided to [Maximus] . . . shall be regarded as confidential information." [See Maximus Reply at 31]. But the CAC contains no allegation that would explain how this contractual language is relevant to the existence of a special relationship within the meaning of New York, Florida, Illinois, or Pennsylvania law.

Finally, Maximus contends that the California, Florida, and Ohio claims suffer the same defect raised by Delta Dental supra, that the CAC lacks any allegation that Maximus "affirmatively shared [] information" or otherwise performed an "act that made [Plaintiffs'] information known." Farmer, 582 F. Supp. 3d at 1189 (first alteration in original) (citation omitted) (Florida law); See also [Maximus Mem. at 52]; accord Ambry, 567 F. Supp. 3d at 1146–47 (same, under California law); Foster v. Health Recovery Servs., Inc., 493 F. Supp. 3d 622, 636 (S.D. Ohio 2020) (under Ohio law, "allegations are not sufficient to state a claim for breach of confidence [if the] [d]efendant did not commit an intentional or unintentional act of disclosure").

Plaintiffs respond that Maximus "acted in a way that made their information available" by using MOVEit and disregarding its security flaws. [Maximus Opp. at 59]. In this iteration, the "act" posited as the basis for Plaintiff's breach of confidence claim is the decision to use MOVEit. Although this argument has some appeal in a metaphysical sense, it is legally insufficient. Even assuming Maximus had known about vulnerabilities in MOVEit and used it anyway, Plaintiffs' argument still falls short under the relevant state law. In Foster, the "alleg[ation] that Defendant was aware of security vulnerabilities but did nothing to remedy those vulnerabilities before an unauthorized third party breached the network" was "not sufficient to state claim for breach of confidence" under Ohio law because that conduct did not amount to "an intentional or unintentional act of disclosure." 493 F. Supp. 3d at 636; accord

Farmer, 582 F. Supp. 3d at 1189 (dismissing claim under Florida law "because there are no alleged facts suggesting that Defendants disclosed Farmer's information to a third party." (cleaned up and citation omitted)); Ambry Genetics, 567 F. Supp. 3d at 1147 ("Since Defendants made no 'disclosure' of Plaintiffs' confidential information, they cannot be held liable on a claim for breach of confidence."). For the foregoing reasons, the motion to dismiss the breach of confidence claim against Maximus is **GRANTED.**

vii. Breach of Contract/Third-Party Beneficiary

Plaintiffs allege the breach of third-party beneficiary contracts as against PBI, Welltok, Delta Dental, and Maximus (but not the VCEs). [CAC ¶¶ 2147–54, 3055–61, 3548–55]. They assert that all PBI Bellwether Defendants entered into contracts "with their government and corporate customers to provide services to them using MOVEit," and that such services "included data security practices, procedures, and protocols to safeguard the PII that was entrusted to" them, [Id. ¶ 2149], see also [Id. ¶ 3057 (similar for Maximus)], that Welltok "entered into written contracts with its Welltok Clients . . . to provide patient engagement services" and "[i]n exchange, Welltok agreed, in part to implement adequate data security measures," [Id. ¶¶ 3548–49]; and Delta Dental contracted with Progress who "agreed to receive, store, utilize, transfer, and protect through their services [Plaintiffs' PII]," [Id. ¶ 2724]. Defendants argue that Plaintiffs' claims are too conclusory to show that Plaintiffs were intended beneficiaries of the contracts. [PBI Mem. at 53–54].

For a third party to recover on a contract claim, the plaintiff must show that he or she was an intended, rather an incidental, beneficiary. Spinner v. Nutt, 631 N.E.2d 542, 546 (Mass. 1994); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 42 (Mass. 2009). The fact that a plaintiff would likely benefit from a contract does not itself render the plaintiff an intended beneficiary. Mass. Eye & Ear Infirmary v. QLT Phototherapeutics, Inc., 412 F.3d 215,

229 (1st Cir. 2005); Rymes Heating Oils, Inc. v. Springfield Terminal Ry., Inc., 265 F. Supp. 2d 147, 151 (D. Mass. 2003). Rather, a plaintiff is considered an intended beneficiary when the "language and circumstances" of the contract indicate a "clear[] and definite[]" intent that the plaintiff would benefit from the promised performance. Mass. Eye & Ear Infirmary, 412 F.3d at 229 (quoting Miller v. Mooney, 725 N.E. 2d 545, 550 (2000)); see also Anderson v. Fox Hill Vill. Homeowners Corp., 676 N.E.2d 821, 822–23 (Mass. 1997). In undertaking this inquiry, "[t]he structure of the performance required under the particular contract often provides the critical indicum of intent in third party beneficiary cases. Unless the performance required by the contract will directly benefit the would-be intended beneficiary, he is at best an incidental beneficiary." Pub. Serv. Co. of N.H. v. Hudson Light and Power Dept., 938 F.2d 338, 343 (1st Cir. 1991) (emphasis omitted).[12]

Although the pleadings are thin, the Court at this stage cannot conclude, without the benefit of seeing the contracts, that Plaintiffs were not intended beneficiaries. See Bennett v. Massachusetts Bay Transp. Auth., No. 93-cv-01409, 1998 WL 52245, at *6 (Mass. Super. Ct. Feb. 2, 1998) (declining to dismiss third party beneficiary claim under Massachusetts law where "[t]he agreement [was] not contained in this record"); Hayes v. CRGE Foxborough, LLC, 167 F. Supp. 3d 229, 244 (D. Mass. 2016) (holding at summary judgment that the court could not "conclude as a matter of law that the contract language or even its terms more generally (if it is an oral contract) bar a third-party beneficiary claim" where the agreement was not in the record); cf. Kroeck v. UKG, Inc., No. 22-cv-00066, 2022 WL 4367348, at *5 (W.D. Pa. Sept. 21, 2022) (holding that, under Pennsylvania law, where "the contract between Defendants and the hospital"

[12] All of the law cited here is First Circuit law, but the parties' briefs cite similar applicable law, and no party has alleged a conflict between any states on any point relevant to this Count.

to which Defendant provided payroll services was not part of the record, the court could not "determine what the contracting parties' expectations were, including whether providing wages to hospital staff was a motivating purpose for contracting with payroll software providers").

As such, PBI's motion to dismiss Count 6, Delta Dental's motion to dismiss Count 10, Maximus's motion to dismiss Count 2, and Welltok's motion to dismiss Count 3 are **DENIED**.

viii. Unjust Enrichment

Plaintiffs claim unjust enrichment against all Non-Progress Defendants. [CAC ¶¶ 2155–60, 2675–90, 3062–74, 3575–94].

Some of the claims fail at the outset. In California, Illinois, and Texas, unjust enrichment does not afford an independent cause of action, a point on which Plaintiffs offer no response. See Cleary v. Philip Morris Inc., 656 F.3d 511, 517 n.2 (7th Cir. 2011) ("The term 'unjust enrichment' is not descriptive of conduct that, standing alone, will justify an action for recovery." (quoting Alliance Acceptance Co. v. Yale Ins. Agency, 648 N.E.2d 971, 977 (Ill. Ct. App. 1995))); Juan Antonio Sanchez, PC v. Bank of S. Tex., 494 F. Supp. 3d 421, 440 & n.135 (S.D. Tex. 2020) (citation omitted) (similar under Texas law); Durell v. Sharp Healthcare, 108 Cal. Rptr. 3d 682, 699 (Cal. Ct. App. 2010) ("There is no cause of action in California for unjust enrichment. Unjust enrichment is synonymous with restitution." (citations omitted)). Similarly, in Florida, North Carolina, New York, Minnesota, Nebraska, and Washington, the pleading of legal remedies precludes pleading unjust enrichment. Alfaro v. Bank of Am., N.A., No. 21-10948, 2024 WL 1110945, at *8 (11th Cir. Mar. 14, 2024), (affirming dismissal of claim under Florida law because plaintiffs alleging "an express contract . . . are not entitled to an unjust enrichment remedy under Florida law"); Corsello v. Verizon N.Y., Inc., 967 N.E.2d 1177, 1185 (N.Y. 2012) (dismissing unjust enrichment claim under New York law because "[a]n unjust

enrichment claim is not available where it simply duplicates, or replaces, a conventional contract or tort claim"); accord Jones Cooling & Heating, Inc. v. Booth, 394 S.E.2d 292, 294 (N.C. Ct. App. 1990); Ahlgren v. Link, No. CV 19-00305, 2019 WL 3574598, at *6 (D. Minn. Aug. 6, 2019); Pilot Inv. Grp. Ltd. v. Hofarth, 550 N.W.2d 27, 33 (Neb. 1996); William Insulation Co. Inc. v. JH Kelly LLC, No. 21-cv-5083, 2021 WL 1894092, at *6 (W.D. Wash. May 11, 2021). This is sufficient to **GRANT** the motion to dismiss Count 6 against Delta Dental.

In Michigan, the fact that the benefit was not "received directly from the [P]laintiff[s]" defeats an unjust enrichment claim. Lochridge v. Quality Temporary Servs., Inc., No. 22-cv-12086, 2023 WL 4303577, at *7 (E.D. Mich. June 30, 2023). This at the very least defeats the claim against Welltok, although not the Welltok VCEs.

As to the remaining claims under Ohio, Indiana, Michigan, Nebraska, North Carolina, Virginia, and Wisconsin law, with some slight variations,[13] "a plaintiff must establish '(1) the receipt of a benefit by the defendant from the plaintiff and (2) an inequity resulting to the plaintiff because of the retention of the benefit by the defendant.'" Lochridge, 2023 WL 4303577 at *6 (quoting Morris Pumps v. Centerline Piping, Inc., 729 N.W.2d 898, 904 (Mich. Ct. App. 2006)); accord Brooks v. Peoples Bank, 732 F. Supp. 3d 765, 782 (S.D. Ohio 2024) (similar under Ohio law); Lindquist Ford, Inc. v. Middleton Motors, Inc., 557 F.3d 469, 477 (7th Cir. 2009) (similar under Wisconsin law), as amended (Mar. 18); Coppolillo v. Cort, 947 N.E.2d 994, 997 (Ind. Ct. App. 2011) (similar under Indiana law); Arch Ins. Co. v. FVCbank, 881 S.E.2d 785, 795 (2022) (similar under Virginia law); Klein v. Klein, No. A-22-241, 2023 WL 367165, at *3 (Neb. Ct. App. Jan. 24, 2023) (similar under Nebraska law); Bandy v. Gibson, No. 16 CVS 456, 2017 WL 3207068 (N.C. Super. July 26, 2017) (similar under North Carolina law).

[13] For example, some of these states also require an appreciation or knowledge of the benefit.

In the MDL Order No. 22, the Court allowed the unjust enrichment claims to proceed because Progress's business "depended on the receipt of [PII]" and therefore the Plaintiffs had alleged that the PII conferred a benefit. That logic is likewise applicable to PBI, Maximus, and Welltok, because their businesses were dependent on collecting and processing Plaintiffs' data for the benefit of the VCEs who contracted with them. The same is not true for the VCEs themselves; while the VCEs may have used the data, it was not central to their businesses. See Webb, 2023 WL 5938606, at *4. The motion to dismiss Count 5 as to the Welltok Bellwether defendants is **GRANTED**. The motion to dismiss Count 7 against PBI is **GRANTED** because there are no claims against PBI itself under the remaining states' laws. The motion to dismiss the unjust enrichment claims against Maximus is **GRANTED** except as to the claims under Ohio, North Carolina, and Indiana law.

ix. Bailment

Delta Dental urges dismissal of Plaintiffs' bailment claim on the ground that California law does not recognize personal information as "property" in the context of a bailment claim. See In re Sony Gaming Networks & Customer Data Sec. Breach Litig. (Sony Gaming I), 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012).

Data breach cases confronting bailment claims under California law all appear to agree with Delta Dental's position. The basis for that uniformity rests in part on the notion that a bailment claim typically involves a return of unlawfully converted property. See Shah v. Cap. One Fin. Corp., 768 F. Supp. 3d 1033, 1052 (N.D. Cal. 2025) ("Plaintiffs do not allege a deposit of personal property that falls within the scope of bailment because they only allege that they deposited their personal information, which is not personal property under bailment."); Worldwide Media, Inc. v. Twitter, Inc., No. 17-cv-07335, 2018 WL 5304852, at *11 (N.D. Cal.

Oct. 24, 2018) (dismissing bailment claim under California law where stolen credit card information "was [not] subject to return to plaintiffs at some later time"); Sony Gaming I, 903 F. Supp. 2d at 974 & n.29 (same, explaining that because "there are no allegations of conversion or any other intentional conduct by Sony that would indicate that Sony sought to unlawfully retain possession of Plaintiffs' Personal Information . . . the Court [was] hard pressed to conceive of how Plaintiffs' Personal Information," and distinguishing examples of unlawfully conveyed funds or internet domain names).

Plaintiffs dedicate only three sentences to their response, with a conclusory assertion that Delta Dental is "wrong that Private Information cannot support a bailment claim" bolstered by a citation to a case applying New York law. This cannot carry the point.[14] [Delta Dental Opp. at 32 (citing Wallace, 2021 WL 1109727, at *14–15)]. The motion to dismiss Count 9 is **GRANTED**.

x. Breach of Fiduciary Duty

Count 11 against Delta Dental, alleges a breach of fiduciary obligations owed to them. The parties dispute whether Plaintiffs' allegations support the existence of a fiduciary relationship with Delta Dental under California law. Plaintiffs contend that "[t]he fiduciary duty arose when DDC mandated that Plaintiffs hand over their Private Information in exchange for coverage for necessary health services." [Delta Dental Opp. at 25]. Delta Dental challenges the existence of a fiduciary relationship on the ground that receipt of confidential information alone does not give rise to fiduciary duties. [Delta Dental Mem. at 39–40]; see also Ambry, 567

[14] Plaintiffs also cite a Ninth Circuit case, Whitcombe v. Stevedoring Servs. Of Am., 2 F.3d 312, 317 (9th Cir. 1993), to suggest that they only needed to "allege that they delivered their Private Information to DDC for safekeeping." [Delta Dental Opp. at 32]. As Delta Dental observes in reply, Whitcombe involved damage to automobiles during shipping, not the theft of data, and does not shed any light on whether personal data constitutes property for purposes of a bailment claim. [Delta Dental Reply at 26].

F. Supp. 3d at 1146 (explaining that "entrust[ing] [d]efendants with their confidential information" in the course of "an arms-length business relationship" does not create a fiduciary relationship). Plaintiffs respond that an insurer with unequal bargaining power who receives confidential information differs from an arms-length business relationship and supports a fiduciary relationship. See [Delta Dental Opp. at 26].

"The question of fiduciary duty is fact-intensive," and thus, the Court focuses on the factual allegations that Plaintiffs cite to support a fiduciary relationship. Prutsman v. Nonstop Admin. & Ins. Servs., No. 23-cv-01131, 2023 WL 5257696, at *1 n.1 (N.D. Cal. Aug. 16, 2023). The CAC includes two such allegations: (1) Delta Dental "became fiduciaries by undertaking a guardianship of the Private Information to act primarily for the benefits of [Plaintiffs]," [CAC ¶ 2730], and (2) Delta Dental "required that [the Plaintiffs] provide their private information" to receive dental insurance, [id. at ¶ 2732]. The first allegation is on shaky ground because, as Delta Dental argues, courts have declined to hold that, under California law, a defendant "bec[o]me[s] a fiduciary by its undertaking and guardianship of PHI/PII" alone. Prutsman, 2023 WL 5257696, at *1.

To be sure, Plaintiffs allege that Delta Dental did not merely receive Plaintiffs' PHI, but "required" them to share PHI in order to obtain insurance services. [CAC ¶ 2732]. This, Plaintiffs contend, reflects the parties' unequal bargaining power [Delta Dental Opp. at 26]. Plaintiffs do not clearly explain, however, why this should affect the analysis under California law. First, although Plaintiffs contend that courts routinely weigh such considerations, Plaintiffs only cite to a single case, which involved a healthcare provider, not an insurer, and a breach of confidence claim under New York law, not a fiduciary duty claim under California law. See Wallace, 2021 WL 1109727, at *13. Whether a medical provider "has a duty to keep confidential

its patients' information" giving rise to a breach of confidence claim, id., presents wholly different questions from whether and under what circumstances an insurer "owes [an] obligation to consider the interests of its insured above its own" so as to support the existence of a fiduciary relationship, Vill. Northridge Homeowners Ass'n v. State Farm Fire & Cas. Co., 237 P.3d 598, 608 (Cal. 2010) (quoting Morris v. Paul Revere Life Ins. Co., 135 Cal. Rptr. 2d 718, 723 (2003)). Second, Plaintiffs cite no California law for the proposition that unequal bargaining power is, in itself, a sufficient condition for finding a fiduciary relationship.[15] Because Plaintiffs have not alleged factual matter to support finding a fiduciary relationship under California law, the motion to dismiss Count 11 against Delta Dental is **GRANTED**.

c. Statutory Claims

i. Statutory standing arguments

The PBI Bellwether Defendants assert that Plaintiffs' Massachusetts, Minnesota, Virginia, Washington, and Wisconsin consumer-protection claims fail because none of the Plaintiffs asserting claims against the PBI Bellwether Defendants is a resident of any of those states and, therefore, lack standing to assert these claims on behalf of other putative class members. This argument is squarely foreclosed by binding First Circuit precedent. "[T]he claims of the named plaintiffs parallel those of the putative class members in the sense that, assuming a proper class is certified, success on the claim under one state's law will more or less dictate success under

[15] California cases in other insurance contexts suggest that Plaintiffs' argument that unequal bargaining power gives rise to a fiduciary relationship between insurers and insureds may fail as a matter of law. Although the insurance relationship is "often characterized by unequal bargaining power," and the California Supreme Court has acknowledged a "special relationship" between insurers and insureds, it has made clear that any "fiduciary-like duties arise because of the unique nature of the insurance contract, not because the insurer is a fiduciary." Vu v. Prudential Prop. & Cas. Ins. Co., 33 P.3d 487, 492 (Cal. 2001) (emphasis in original) (quoting Love v. Fire Ins. Exch., 271 Cal. Rptr. 246, 253 (1990)).

another state's law." In re Asacol Antitrust Litig., 907 F.3d 42, 49 (1st Cir. 2018). "[O]nce the named plaintiff establishes injury and membership in the class, the inquiry should shift 'from the elements of justiciability to the ability of the named representative to "fairly and adequately protect the interests of the class."'" Id. at 51 (quoting Sosna v. Iowa, 419 U.S. 393, 393 (1975)). To the extent that material differences between the laws of the states where Plaintiffs reside and the laws of Massachusetts, Minnesota, Virginia, Washington, and Wisconsin would prevent class certification, they should not be litigated on the pleadings, particularly since Defendants have not yet identified such differences. "[A]t the motion-to-dismiss stage, Plaintiffs need only plausibly allege that they can establish the elements of standing" consistent with Article III, In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014), which the Court found are satisfied here in its earlier order on standing.

ii. Massachusetts General Laws Chapter 93A

Plaintiffs allege that all Bellwether Defendants (except the Welltok VCEs[16]) are liable under Chapter 93A, as alleged in Count 8 against the PBI Bellwether Defendants, Count 23 against Delta Dental, Count 13 against Maximus, and Count 16 against Welltok.

The Bellwether Defendants make several arguments for dismissal of the 93A claims. First, Delta Dental, Maximus, and Welltok each contend that the allegations did not occur "primarily and substantially" in Massachusetts, as required by the statute.[17] Mass. Gen. Laws.

[16] Plaintiffs have expressly abandoned their Chapter 93A claims against the Welltok VCEs. [Welltok Opp. at 64].

[17] Relatedly, Delta Dental offers a confusing argument that the scope of a Chapter 93A claim is "governed by the Massachusetts longarm statute." [Delta Dental Mot. at 78-79]. The cases Delta Dental cites, however, discussed the Massachusetts long-arm statute only in that statute's intended context, i.e., the sufficiency of a court's personal jurisdiction, not for the purpose of importing any additional requirement under Chapter 93A. See Snyder v. ADS Aviation Maint., No. 9700968, 2000 WL 145110, at *7 (Mass. Super. Jan. 10, 2000); Source One Fin. Corp. v. Omni Ins. Grp., 2011 Mass. App. Div. 142, 2011 WL 2449510, at *4 (Mass. App. Ct. June 17, 2011).

ch. 93, § 11. As the Court explained with respect to Progress's similar argument, it is important to consider which section of Chapter 93A is at issue. Claims under § 11 must allege that the "center of gravity" of "the unfair and deceptive conduct" was "primarily and substantially within the Commonwealth," HC&D, LLC v. Precision NDT & Consulting LLC, No. 22-cv-10224, 2024 WL 4626223, at *7 (D. Mass. Oct. 30, 2024) (first quoting Sonoran Scanners, Inc. v. PerkinElmer, Inc., 585 F.3d 535, 546 (1st Cir. 2009), next quoting Arthur D. Little v. Dooyang, Corp., 147 F.3d 47, 52 (1st Cir. 1998), and then quoting Sonoran, 585 F.3d at 546). Here, however, Plaintiffs bring their claims under § 9 of the statute and that section provides a private right of action to "individual consumers who have suffered a loss due to an unfair trade practice whereas section 11 pertains to persons acting in a business context." Iron Workers Dist. Council of New Eng. Health & Welfare Fund v. Teva Pharm. Inc., 734 F. Supp. 3d. 145, 162 (D. Mass. 2024) (emphasis added). Unlike § 11, §9 does not include the kind of nexus requirement that Defendant's rely on. Thus, without more, the objections on this ground do not support dismissal.

Next, the PBI Bellwether Defendant argues that Plaintiffs' allegations are "boilerplate claims of 'unfair' practices" that only offer a conclusory recitation of the applicable legal standard. See [PBI Mem. at 68]. Maximus similarly suggests that the allegations here do not state a claim for unfair conduct. [Maximus Mem. at 75–76]. This argument rests on a blinkered view of the CAC; PBI's argument addresses only the allegations recited in the specific count alleged against it, see [CAC ¶¶ 2164–75], to the exclusion of the CAC's broader allegations against it, which the Chapter 93A count incorporates by reference. [Id. ¶ 2161]. The Court agrees with Plaintiffs that their allegations of inadequate security protocols, which the Court must take as true at this stage, are akin to the allegations of "unreasonably weak internal and external cybersecurity protocols" in LastPass, which stated a claim under Chapter 93A. In re

LastPass Data Sec. Incident Litig., 742 F. Supp. 3d 109, 131 (D. Mass. 2024). An alleged "lack of security measures," particularly in light of the allegation that there was a failure to implement industry-standard security measures, states a claim for an unfair practice under Chapter 93A. In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496 (1st Cir. 2009).

Maximus and Welltok also argue that Plaintiffs do not plead economic damages. [Maximus Mem. at 80–81]; [Welltok Mem. at 76–77]. A plaintiff alleging a Ch. 93A violation "must 'show "real" economic damages,' as opposed to some speculative harm." Shaulis v. Nordstrom, Inc., 865 F.3d 1, 10 (1st Cir. 2017) (quoting Rule v. Fort Dodge Animal Health Inc., 607 F.3d 250, 253 (1st Cir. 2010)); see also Young v. Wells Fargo Bank, N.A., 717 F.3d 224, 241 (1st Cir. 2013) (explaining that "[c]ase law on the types of damages that are cognizable under Chapter 93A continues to evolve"). Here, not only do Plaintiffs allege that they have suffered monetary losses in the form of fraudulent charges, but they also allege that they will suffer difficulties managing their identity and financial accounts due to past and future identity theft, and that they have lost the value of their PII. [CAC ¶¶ 34, 40, 58, 76, 88, 95, 113, 131, 143, 167, 184, 218]. Drawing reasonable inferences in Plaintiffs' favor, these allegations seek cognizable economic damages within the scope of Chapter 93A. See Young v. Wells Fargo Bank, N.A., 717 F.3d 224, 241–42 (1st Cir. 2013) (holding that monetary injuries or difficulty accessing credit constituted economic damages that "adversely affect [plaintiff] now and will continue to affect her in the future"); cf. Rule, 607 F.3d at 255 (affirming dismissal under Ch. 93A where Plaintiff "neither h[eld] nor sold anything of reduced value, faced no continuing risk and suffered no harm").

Delta Dental also argues that Plaintiffs failed to provide the notice required under the statute. Chapter 93A section 9(3) requires that "[a]t least thirty days prior to the filing of any

such action, a written demand for relief, identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered, shall be mailed or delivered to any prospective respondent." Mass. Gen. Laws ch. 93A, § 9(3). Plaintiffs suggest there is reason to think that Delta Dental was on notice of the Chapter 93A claims as early as June 2024. See [Delta Dental Opp. at 62].[18] Even if that were not the case, they allege they sent demand letters to Delta Dental on December 6, 2024, which satisfies the statutory requirement at least with respect to the filing of the corrected CAC. [Delta Dental Opp. at 62; CAC ¶ 2811]. As Delta Dental's own cases explain, this should be enough:

> A failure to allege compliance with the statutory notice requirement is not necessarily a death knell for a Chapter 93A claim. Massachusetts courts typically have allowed plaintiffs to amend in order to cure this kind of modest pleading defect. Federal practice is no less permissive.

Rodi, 389 F.3d at 20 (citations omitted). Here, the corrected pleadings were filed in compliance with the statutory notice requirements, and the Court declines to dismiss potentially meritorious claims on that ground alone.

Finally, to the extent Maximus contends that Plaintiffs needed to plead actual reliance or that the alleged security practices do not qualify as "unfair" under Chapter 93A, the Court disagrees. See [Maximus Mem. at 71]. "[U]nlike a traditional common law action for fraud, consumers suing under [chapter] 93A need not prove actual reliance on a false representation . . . ." In re M3 Power Razor Sys. Mktg. & Sales Prac. Litig., 270 F.R.D. 45, 60 (D. Mass. 2010)

[18] As Plaintiffs explain, "[m]any of the same Bellwether Plaintiffs here further notified DDC of their claims under 93(A) and their demand for relief in a complaint filed against DDC on June 12, 2024." [Delta Dental Opp. at 62]. Although the Court is skeptical of Plaintiffs' suggestion that the filing of a complaint constitutes pre-suit notice, it undeniably made Delta Dental aware of potential Chapter 93A liability more than six months before the filing of the operative allegations.

(quoting Dalis v. Buyer Advert., Inc., 636 N.E.2d 212, 216 (Mass. 1994)); see also Slaney v. Westwood Auto, Inc., 322 N.E.2d 768, 779 (Mass. 1975) ("[P]roof of actual reliance by the plaintiff on a representation is not required."). Maximus cites no case to the contrary. [Maximus Mem. at 71].[19]

The motions to dismiss the Chapter 93A claims are **DENIED**.

iii. California Consumer Privacy Act

The Plaintiffs allege that PBI and Genworth (in Count 11), Maximus (in Count 8), and Welltok (in Count 7) are liable under the California Consumer Privacy Act ("CCPA"). The CCPA imposes a duty on businesses that collect or maintain a Californian's "personal information" to "implement and maintain reasonable security procedures and practices," Cal. Civ. Code § 1798.81.5(b), and confers a private right of action for "consumers" whose "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of th[at] duty," id. § 1798.150(a)(1).

PBI, Genworth, Maximus, and Welltok urge dismissal on several grounds. First, PBI, Maximus and Welltok (but not Genworth) dispute whether they qualify as a "business" under the statute. The CCPA defines a "business" in relevant part as:

> [A] legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information.

[19] Maximus also suggests that Plaintiffs have failed to plead causation, but only cites summary judgment cases. See Walsh v. TelTech Sys., Inc., 821 F.3d 155, 160 (1st Cir. 2016). They offer no convincing ground as to why the Plaintiffs' allegations that stronger security procedures would have prevented the Data Breach are inadequate at this stage.

Cal. Civ. Code § 1798.140(d)(1). Thus, "for an entity to be a 'business' under the CCPA, it must: '(1) collect PII and (2) determine why and how ("the purposes and means") the PII should be processed.'" Miller v. NextGen Healthcare, Inc., 742 F. Supp. 3d 1304, 1327 (N.D. Ga. 2024) (quoting Accellion, 713 F. Supp. 3d at 640). PBI, Maximus, and Welltok attack the second prong, arguing that the allegations establish only that they are "service provider[s]" because they "process[] personal information on behalf of a business" and receive information "for a business purpose pursuant to a written contract." Cal. Civ. Code § 1798.140(ag)(1).

The Court has no basis to conclude that the defendants are service providers rather than businesses.[20] Defendants overlook that a service provider is not just any person processing information received from a business; rather, the contract must "prohibit[] the person from," inter alia, "using . . . the personal information for any purpose other than for the business purposes specified in the contract." Cal. Civ. Code § 1798.140(ag)(1)(B). Prior to discovery, the Court cannot determine whether those contractual limitations, or others required by statute, are present in the relevant contracts and declines to draw that inference in Defendants' favor on a motion to dismiss.

[20] Plaintiffs propose that the Defendants can be both service providers and businesses under the statute, so they can pursue a claim against the Defendants even if they satisfy the former definition, so long as they also satisfy the latter. The limited case law on the question, however, appears to be split, and the Court declines to weigh in on it unnecessarily. Compare In re NCB Mgmt. Servs. Inc. Data Breach Litig., 748 F. Supp. 3d 262, 288 (E.D. Pa. 2024) (holding service providers and businesses are not mutually exclusive), and In re Blackbaud, Inc., Customer Data Breach Litig., No. 20-mn-02972, 2021 WL 3568394, at *5–6 (D.S.C. Aug. 12, 2021) (allowing claim to proceed against service provider who also qualified as a "business"), with Kanter v. Epic Sys., Inc., No. SACV 20-01385, 2021 WL 4353274, at *2 (C.D. Cal. 2021) ("Plaintiff can only state a claim against Defendants if they are businesses, not service providers" because CCPA enforcement actions against service providers may only be brought "by the [California] Attorney General." (citation omitted)).

Further, whether Plaintiffs have sufficiently alleged that Defendants are "businesses" varies among the Defendants. Plaintiffs do allege that PBI collects PII and makes decisions about data processing. In the course of death-matching, "PBI and Genworth collect PII" and "determine which PII to retain or transfer, where and how to store it, and how to search and process the information according to their business needs, among other decisions." [CAC ¶ 2203]. Similarly, Plaintiffs allege that Welltok makes data-processing determinations when it analyzes health data to tailor consumer-activation services to its customers. [Id. ¶¶ 3300–05]. As to Maximus, however, the CAC lacks similar allegations about the data-processing decisions apart from conclusory recitations of the statutory definition. [Id. ¶ 3135]; In re NCB Mgmt. Servs., Inc. Data Breach Litig., 748 F. Supp. 3d 262, 288 (E.D. Pa. 2024) ("The complaint lacks any allegations about 'determinations' that NCB made regarding why and how the plaintiffs' PII was to be processed. The allegation that NCB used their PII to provide its debt collection services to the Bank Defendants is a far cry from alleging it played any role in determining how to process the plaintiffs' PII."). Thus, Maximus's motion to dismiss Count 8 is **GRANTED**, and the Court need not reach Maximus's other proffered grounds for dismissal.

Welltok and PBI further contend that the CCPA claims should be dismissed for inadequate pre-suit notice, which Plaintiffs provided only in November of 2024. [Welltok Opp. at 46; PBI Opp. at 63]. For reasons similar to the Chapter 93A notice decision, supra, the Court finds that notice is adequate.

PBI and Welltok also claim that Plaintiffs fail to plead facts sufficient to show that the MOVEit incident occurred as a result of either PBI's or Genworth's violations of the duty to implement and maintain reasonable security procedures and practices. [PBI Mem. at 70; Welltok Mem. at 55–56]. For similar reasons as finding breach under the negligence claims, the

Court declines to grant dismissal on this ground. Plaintiffs plead that this specific breach could not have occurred but for Defendants' failure to take certain preventative steps; rather than pleading a per se injury generally. See, e.g. [CAC ¶¶ 1979–80]. That is sufficient.

Furthermore, the PBI Bellwether Defendants claim that PBI and Genworth notified Plaintiffs that the vulnerability was fixed, "cur[ing]" the violation under Cal. Civ. Code § 1798.150(b), and therefore preventing statutory damages. [PBI Mem. at 71]. Curing requires "an express written statement that the violations have been cured and that no further violations shall occur." Cal. Civ. Code § 1798.150(b). Plaintiffs counter that this notice was insufficient because it failed to specifically identify the actions that either party took to cure beyond bare assertions. [PBI Opp. at 62]. Importantly, as Plaintiffs identify, "the implementation and maintenance of reasonable security procedures and practices" is insufficient to constitute a cure under the CCPA. Florence v. Ord. Express, Inc., 674 F. Supp. 3d 472, 483 (N.D. Ill. 2023) (internal quotation omitted). The case that Plaintiffs cite, however, is distinguishable from the present case. In that case, Defendant "claimed to have enhanced its security measures." Id. Here, by contrast, Plaintiffs acknowledge that PBI and Genworth stated in their letter that PBI had implemented the patches sent by Progress. [PBI Opp. at 62]. Given that implementing the patches is precisely what Plaintiffs say would have prevented the breach, the Court holds that this is sufficiently specific to constitute a statement that the violation has been cured. Therefore, PBI Bellwether Defendants' motion to dismiss Count 11 is **GRANTED**. However, Welltok's motion to dismiss Count 7 is **DENIED**.

iv. California Customer Records Act

The California Customer Records Act ("CCRA") claims against Maximus, Welltok, and PBI all fail because none of the California Plaintiffs are "customers" of those Defendants. "Any customer injured by a violation of [the CCRA] may institute a civil action to recover damages,"

Cal. Civ. Code § 1798.84(b), and "customer" is defined under the statute as "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business," id. § 1798.80(c). The allegations make clear that the Plaintiffs are customers of Genworth and Sutter Health and provided their data to those companies, not to PBI or Welltok. E.g., [CAC ¶ 264 ("Plaintiff Copans is a current patient at Sutter Health, which . . . contracted with Welltok.")]. Nor do the allegations suggest that any Plaintiff provided "personal information" to Maximus "for the purpose of purchasing or leasing a product or obtaining a service from" Maximus. Cal. Civ. Code § 1798.80(c). Rather, the CAC alleges that "[a]s a condition of performing its services," Maximus's "government and corporate customers," not Plaintiffs, "entrust it with highly sensitive Private Information." [CAC ¶ 2934]. Courts routinely refuse to find that plaintiffs are customers under the CCRA where "[t]here are no allegations [they] paid money or obtained any service from [the defendant]." Accellion, 713 F. Supp. 3d at 645; see also Toretto v. Donnelly Fin. Sols., Inc., 583 F. Supp. 3d 570, 603 (S.D.N.Y. 2022) (finding plaintiff was not "customer" under CCRA because complaint alleged defendant obtained plaintiff's data "while providing services to an entity in which [plaintiff] had invested"); Miller, 742 F. Supp. at 1321 (N.D. Ga. 2024) (same, where "the California Plaintiffs did not provide their private information to NextGen in exchange for NextGen's software or services," but "[r]ather, they were required to do so as patients of their healthcare providers").

That leaves Delta Dental, Genworth, and Sutter Health.[21]

Genworth challenges Plaintiffs' allegation that it is liable under the CCRA because it "failed to disclose the MOVEit incident in a timely manner." [PBI Mem. at 72]. The Court

[21] Because Sutter Health and Delta Dental are HIPAA-covered entities, they are exempted from the CCRA's "reasonable security measures" provision and only required to comply with the breach-notification provisions.

agrees. According to the Complaint, PBI notified Genworth on June 16, 2023 that files containing policyholder information had been impacted in the Data Breach, [CAC ¶ 1901]. Plaintiffs allege that Genworth "waited . . . two weeks before they informed impacted individuals . . . that their sensitive PII was involved in the Data Breach," [id. ¶ 1902], saying that they received notice on July 21 and/or 31, 2023, [id. ¶¶ 680–81, 698–99, 750, 802]. Genworth contends that two to six weeks of elapsed time between learning of the breach and notifying impacted individuals provides "no basis for holding that there was any delay in notifying Plaintiffs . . . after determining the extent to which Plaintiffs' personal information may have been impacted." [PBI Mem. at 72–73]. Genworth also observes that public company materials cited in the CAC explain that Genworth "promptly launched an investigation to determine to what extent personal information had been unlawfully accessed by the threat actor," [PBI Mem. at 72 (citing document cited at CAC ¶ 1903 n.551)].[22]

Rather than dispute Genworth's reading of the Complaint, Plaintiffs contend that, at this stage, the Court must take at face value their assertion that the delay was unreasonable. [PBI Opp. at 64 & n.118 (citing cases)]; e.g., Ambry, 567 F. Supp. 3d at 1150 (accepting "as true" allegations that a "3-month delay was unreasonable"). The Court does not take issue with the decisions that Plaintiffs cite, although it is worth noting that in each case cited by Plaintiffs the delays were somewhat longer than the time it took Genworth to give notice. Ambry, 567 F. Supp. 3d at 1150 (three months); LastPass, 742 F. Supp. 3d at 129 (four months); In re Fortra

[22] On a motion to dismiss pursuant to Rule 12(b)(6), the Court may consider "'implications from documents' attached to or fairly 'incorporated into the complaint,'" Schatz v. Republican State Leadership Committee, 669 F.3d 50, 55 (1st Cir. 2012) (citation omitted), and "the documents may trump the complaint's allegations if a conflict exists," id. at 55 n.3 (citation omitted).

File Transfer Software Data Sec. Breach Litig., 749 F. Supp. 3d 1240, 1263 (S.D. Fla. 2024) (two months).[23]

The problem here is the dearth of factual allegations to support Plaintiffs' claim that any particular period of time—days, weeks, or months—amounts to an unreasonable delay and on its face, the amount of time here does not appear to be unreasonable. Context is critical: Was the delay attributable to difficulties in identifying what information was compromise? Or was the Defendant sitting on known information for no good reason? When it comes to pleading a viable claim, "[a] plaintiff is not entitled to proceed perforce by virtue of allegations that merely parrot the elements of the cause of action." Ocasio-Hernandez, 640 F.3d at 12 (internal quotation marks and citation omitted). Though the reasonableness of a delay surely involves questions of fact, Plaintiffs' mere allegation that the notification was untimely, [CAC ¶ 2218], is conclusory at best, particularly in light of the foregoing—apparently undisputed—factual allegations in the Complaint concerning the timing of Genworth's notice and the actions it was taking during that period. Data breach notices do not, and cannot, happen in a vacuum. Even the text of the CCRA recognizes that the duty to disclose "without unreasonable delay" is tempered by the reality that some lapse in time is inevitable. Cal. Civ. Code § 1798.82(a) (requiring expedient disclosure "consistent with . . . any measures necessary to determine the scope of the breach"). Here, taking all facts alleged by the Plaintiff as true, the Court does not find a two- to-six week delay during which time Genworth was taking "measures necessary to determine the scope of the breach"

[23] Plaintiffs also cite Smallman v. MGM Resorts International, 638 F. Supp. 3d 1175, 1205 (D. Nev. 2022), but that decision did not appear to involve a delayed-notice claim. It addressed the different CCRA violation of retaining PII "for longer than was necessary." Id.; see also Cal Civ. Code § 1798.81.

could plausibly be interpreted as "unreasonable," despite Plaintiff's conclusory allegations that the delay was unreasonable. Id.

The allegations against Sutter Health similarly falter. Plaintiffs concede that only one month passed between when Welltok informed Sutter Health of the breach, and when Sutter Health disclosed the breach to affected patients. [Welltok Opp. at 53]. The Complaint indicates that Sutter Health's notice to patients was sent on October 31, 2023, which was only seven days after it received a final investigative report. [CAC ¶¶ 3469, 3478]. These allegations do not support a plausible inference that Sutter Health's conduct was unreasonable and was not justified by the need to investigate the scope of the breach.

That leaves just Delta Dental, which contends that the California Plaintiffs have not alleged an incremental harm proximately caused by the delay, rather than by the data breach itself. The Court agrees.

As explained above, the CCRA requires that entities doing business in California disclose covered data breaches to affected California residents "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). "To allege a 'cognizable injury' arising from delay, a plaintiff must allege 'incremental harm suffered as a result of the alleged delay in notification,' not merely the data breach itself." In re Mednax Servs., Inc., Customer Data Sec. Breach. Litig., 603 F. Supp. 3d 1183, 1219 (S.D. Fla. 2022) (quoting Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 16-cv-00014, 2016 WL 6523428, at *7 (S.D. Cal. Nov. 3, 2016)); In re Sony Gaming Networks & Customer Data Sec. Breach Litig. (Sony Gaming II, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) ("[P]laintiff must allege actual damages flowing from the unreasonable delay (and not just the intrusion itself)."); In re Yahoo! Inc.

Customer Data Sec. Breach Litig., No. 16-md-02752, 2017 WL 3727318, at *40 (N.D. Cal. Aug. 30, 2017) (same).

Plaintiffs say that but for those delays, they would have "taken additional precautions earlier on to protect [their] identit[ies] and mitigate the harms of the Data Breach," chiefly by setting up fraud monitoring sooner. E.g., [Delta Dental Opp. at 49]. They say that "[c]ourts applying the [C]CRA have inferred from plaintiffs' post-disclosure remedial actions—coupled with allegations of harm by the data breach—that timely disclosure would have prompted a swifter response and that the delay caused the type of cognizable injury—i.e., ongoing compromise of unprotected data—required by the statute." [Delta Dental Opp. at 34 (quoting Mednax, 603 F. Supp. 3d at 1219 (citing Yahoo!, 2017 WL 3727318, at *41))].

Delta Dental responds that these alleged harms "lack clear mitigation potential and fail to link delayed notification to exacerbated harms." [Delta Dental Reply at 38]. The harms involved in Mednax included that a plaintiff's "credit score ha[d] been damaged, that she ha[d] experienced errors in processing her medical bills, and that a four-year magazine subscription was started in her name." 603 F. Supp. 3d at 1201. Such specific harms are materially distinct from "allegations of increased spam, lost time, and anxiety" and lost opportunity to mitigate a risk of future identity theft sooner. [Delta Dental Reply at 38 (citing CAC ¶¶ 451, 453, 457, 461, 570–71, 575, 578)].

The Court therefore agrees with Delta Dental. Although Plaintiffs are correct that courts have inferred incremental harm from a lost opportunity to mitigate damages, those cases support Delta Dental's argument that such damages must be susceptible to mitigation. See Yahoo!, 2017 WL 3727318, at *41 ("As a result of these Data Breaches, Plaintiffs Heines and Dugas experienced fraudulent charges on their accounts and fraudulent tax returns filed in their names,

which resulted in harm to their credit scores and hours spent talking to the police, banks, and businesses . . . . A reasonable inference from these allegations is that if Plaintiffs had been aware of the Data Breaches a year to two years earlier, Plaintiffs could have taken earlier measures to mitigate the harms that they suffered from the Data Breaches."); Mednax, 603 F. Supp. 3d at 1201 (reviewing plaintiffs' allegations including one plaintiff who alleged "that she ha[d] suffered identity theft, that twelve bank accounts ha[d] been opened in her name, that her credit score ha[d] been damaged, that she ha[d] experienced errors in processing her medical bills, and that a four-year magazine subscription was started in her name") Plaintiffs have not alleged damages of the kind listed in Yahoo!, such as fraudulent charges and tax returns that are susceptible to mitigation.

v. California Unfair Competition Law

PBI and Genworth argue that Plaintiffs cannot seek relief under the California Unfair Competition Law ("CUCL"), because they have not established entitlement to injunctive relief, as is required. Weizman v. Talkspace, Inc., 705 F. Supp. 3d 984, 989 (N.D. Cal. 2023) ("Remedies under the UCL are equitable in nature and legal damages cannot be recovered."). Plaintiffs properly characterize that ruling, however, as limited to the adequacy of injunctive relief against Defendants to protect Plaintiffs from future misuse of the data Cl0p has already stolen. [PBI Opp. at 80–81]. That is different from the request for injunctive relief Plaintiffs assert here, which addresses the risk of a separate, future data breach due to ongoing deficiencies in PBI's cybersecurity program. Plaintiffs specifically allege that PBI has not improved its cybersecurity, [CAC ¶ 2128] and continues to possess Plaintiffs' data, [id.]. In light of these allegations, the Court declines to foreclose such relief at this stage. Cf. In re Arby's. Rest. Grp. Inc. Litig., No. 17-cv-0514, 2018 WL 2128441, at *15 (N.D. Ga. Mar. 5, 2018) ("Arby's arguments are premature at this stage. Plaintiffs made specific allegations that they would be

harmed without declaratory relief because Arby's has not taken steps to address their allegedly inadequate security system. This is enough to survive a motion to dismiss.").

PBI additionally argues that federal courts require remedies at law to be unavailable in order for injunctive relief to be available under the CUCL. [PBI Mem. at 73–74]. Plaintiffs counter that, where the past harm and future harm are distinct, courts have allowed both. [PBI Opp. at 65 (citing Zeiger v. WellPet LLC, 526 F. Supp. 3d 652, 687 (N.D. Cal. 2021)]. Such is the case here; as with the standing discussion, Plaintiffs seek legal remedies for the past harms, i.e. the Cl0p breach; and injunctive relief for distinct possibilities of future harms, i.e. the risk of future breaches given that Defendants still possess their data. See Zeiger 526 F. Supp. 3d at 687.[24]

Finally, PBI argues that Plaintiff either needs to meet 9(b) pleading requirements or establish violations of either the CCPA or CRA to show "fraudulent," "unfair," or "unlawful" conduct as required under the CUCL. Lambrix v. Tesla, Inc., 737 F. Supp. 3d 822, 851 (N.D. Cal. 2024). While this may be true of allegations that sound in fraud, an alleged lack of security measures, especially the industry-standard security measures alleged here, can state a claim for an unfair practice under CUCL. Hameed-Bolden v. Forever 21 Retail, Inc., No. CV 18-03019, 2018 WL 6802818, at *7–8 (C.D. Cal. Oct. 1, 2018). Therefore, PBI's motion to dismiss Count 13 is **DENIED**.

Maximus argues that there is an insufficient nexus between the conduct and California. [Maximus Mem. at 61 (citing In re NCB Mgmt. Servs., Inc. Data Breach Litig., No. 23-1236, 2024 WL 4160349, at *14 (collecting cases) ("In all data breach cases . . . application of the

[24] Maximus makes a similar argument in a footnote, [Maximus Mem. at 82 n.37], and it is denied for similar reasons.

UCL has been allowed only when the liability-causing conduct emanated from California.")]. However, because Plaintiff McCaskell is a California resident, this argument fails. See Norwest Mortg., Inc. v. Super. Ct., 72 Cal. App. 4th 214, 222 (1999). Maximus also makes the same 9(b) argument as PBI; this likewise fails because Plaintiffs sufficiently allege unfair acts, i.e., a lack of security measures. Hameed-Bolden, 2018 WL 6802818 at *4.[25]

Furthermore, Maximus argues that Plaintiffs have not shown the economic injury necessary for a UCL claim. [Maximus Mem. at 79]. However, under the CUCL, "Plaintiffs' allegation that the value of their personal information has diminished is also sufficient to state an injury." Owens v. Smith, Gambrell & Russell Int'l, LLP, No. LA CV23-01789, 2024 WL 3914663, at *14 (C.D. Cal. May 30, 2024). Therefore, the motion to dismiss Count 11 against Maximus is **DENIED**.

Delta Dental argues (1) Plaintiffs are not entitled to equitable relief; (2) Plaintiffs do not meet the 9(b) pleading standard, and (3) Plaintiffs' CUCL claim "lumps" DDC and DDA together. [Delta Dental Mem. at 75–77]. For the same reasons as discussed supra, the Court rejects the first argument. As to the second, for the same reasons as discussed for PBI, the Court rejects this argument insofar as Plaintiffs allege an unfair practice in the form of inadequate data security. And because the more liberal pleading standard applies, the Court holds that the Complaint's allegations of inadequate security as against both parties, [CAC ¶ 2776], are sufficient. Therefore, the motion to dismiss Count 15 against Delta Dental is **DENIED**.

[25] Maximus argues that an unfairness allegation cannot survive because it overlaps totally with the misrepresentation allegations. [Maximus Mem. at 75]. The Court disagrees; the failure to maintain private information is a distinct theory of liability from the failure in connection with a misrepresentation or omission, as is relevant for the fraud claims.

Welltok and Sutter Health raise no new arguments, claiming that equitable relief is unavailable and that Plaintiffs have inadequately alleged harm. For the reasons already articulated as to the other Defendants, the motion to dismiss Count 10 against Welltok is **DENIED**.

vi. California Legal Remedies Act

The California Legal Remedies Act ("CLRA") makes it unlawful for a business to make misleading representations about its products or services. Cal. Civ. Code § 1770(a). The CLRA prohibits unfair methods of competition and unfair practices "undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer." Id. § 1770(a).

Plaintiffs raise the CLRA only against Genworth as to the PBI Defendants, as all California Plaintiffs are annuitants or policyholders with Genworth. [PBI Mem. at 74]. Defendant argues that the CLRA does not apply to Genworth because it only applies to "goods or services," of which insurance and annuities are neither. Cal. Civ. Code § 1770(a); [PBI Mem. at 53]. Plaintiffs argue that this restriction does not apply, because they are not alleging a problem with the insurance policies themselves. [PBI Opp. at 66].

Plaintiffs' argument is puzzling, because it does not address the fact that the transactions at issue, regardless of whether the conduct was as to the policies themselves or the maintenance of data, were not "intended to result . . . in the sale or lease of goods or services." Cal. Civ. Code § 1770(a). For that reason, the PBI Defendants' motion to dismiss Count 14 is **GRANTED**.

Welltok and Sutter Health make different arguments. First, Welltok and Sutter Health both argue inadequate notice. For the same reasons as the 93A claim discussed supra, the Court finds the notice adequate. Second, Welltok argues that Plaintiffs did not engage in a transaction with Welltok. [Welltok Mem. at 67]. Plaintiffs respond that indirect transactions can suffice for

a CLRA claim. [Welltok Opp. at 58]. The Court agrees with Welltok that Plaintiffs have not, as required, pled an indirect transaction that would support a CLRA claim. Hammerling v. Google LLC, 615 F. Supp. 3d 1069, 1087 (N.D. Cal. 2022) ("Although courts have held that the CLRA does not require a direct transaction between a plaintiff and a defendant, in cases where there was no direct sale, the plaintiff sued either (1) the manufacturer of the product or (2) a party that received some portion of the product's sale . . . . Plaintiffs claim in their brief that Google receives a portion of the sale of the smartphones, . . . but they do not do so anywhere in their complaint." (citation omitted)). Likewise here, the CAC alleges only that Welltok "would be unable to engage in their regular business activities without collecting and aggregating Private Information" which is insufficient. [CAC ¶ 3319]; see also [Welltok Opp. at 58–59 (citing CAC ¶ 3319 for the proposition that "Plaintiffs allege that Welltok receives a portion of the monies paid by Plaintiffs to their healthcare providers for the provision healthcare services as Welltok's business would not exist but for the need to collect and aggregate Plaintiffs' Private Information.")]. Thus, the motion to dismiss CLRA claim against Welltok is **GRANTED**.

As to Sutter Health, Defendant argues that Plaintiffs have not alleged reliance and have not met the Rule 9(b) pleading burden. [Welltok Mem. 67]. Plaintiffs counter that, because they are claiming a fraudulent omission, the 9(b) standard is relaxed, and Plaintiffs need only establish that Defendant had a duty to disclose and that, had the information been disclosed, Plaintiffs would have acted differently. [Welltok Opp. at 57]. They argue that Sutter Health had a duty based on "exclusive knowledge of the alleged inadequacy of its security measures." [Id.] Defendant rejoins that Sutter Health could not have had exclusive knowledge of a zero-day vulnerability. [Welltok Reply at 27]. Because Sutter Health is a VCE and not a direct user of the MOVEit software, Defendant has the better argument. Even as we have held that Plaintiffs

have adequately alleged the direct users had knowledge of their failures to take steps that would have prevented the vulnerability, all Plaintiffs allege with regard to the VCEs is that they did not adequately vet their vendors. [Welltok Opp. at 32 (citing CAC ¶¶ 3428, 3430, 3511)]. This is distinct from "exclusive knowledge" that there was, in fact, a security vulnerability. Thus, the motion to dismiss Count 8 as against Sutter Health is **GRANTED**.

Finally, Delta Dental makes arguments similar to the other Defendants. As a threshold matter, DDA argues that it does not provide and has never provided dental insurance to Bellwether Plaintiffs, and therefore, like Genworth, there is no "transaction intended to result or that results in the sale or lease of goods or services to any consumer." Cal. Civ. Code § 1770(a); [Delta Dental Mem. at 75]. Plaintiff makes no argument to the contrary and focuses its opposition entirely on DDC. Therefore, the motion to dismiss Count 17 is **GRANTED** as to DDA.

As to DDC, Defendants argue that Plaintiffs have not met the 9(b) pleading standard because they have not pled reliance, and that they do not adequately distinguish between DDC's and DDA's actions, or plead facts demonstrating causation. [Delta Dental Mem. 52–53]. Plaintiffs respond that, under an omission theory, Rule 9(b) is "somewhat relaxed" and omission can be established by presumption if the defendant had a duty to disclose. [Delta Dental Opp. at 52–53 (quoting Montich v. Miele USA, Inc., 849 F. Supp. 2d 439, 451 (D.N.J. 2012)]. As DDC notes in its reply, to the extent that Plaintiffs' original allegations indicated a theory of intentional fraud, Plaintiffs have seemingly abandoned that theory. However, Defendants' remaining arguments regarding reliance do not address Plaintiffs' omission theory; indeed, they cite language in In re Anthem, Inc. Data Breach Litig. that refers to intentional misrepresentations in holding that the plaintiffs' allegations of reliance were too conclusory. No.

15-MD-02617, 2016 WL 3029783 at *37–38 (N.D. Cal. May 27, 2016). Here, by contrast, the Court agrees that it is sufficient that Plaintiffs have alleged Defendants had "exclusive knowledge of the alleged inadequacy of its security measures" that it failed to disclose. This is likewise sufficient for causation. Red v. Kraft Foods, Inc., No. CV 10–01028, 2012 WL 8019257, at *7 (C.D. Cal. Apr. 12, 2012) ("As for Plaintiffs' CLRA claims, while individualized reliance (i.e. causation) is an element of a CLRA claim . . . if there have been material misrepresentations made to the entire class, then the Court will infer a presumption of reliance as to the class, and individualized causation need not be shown"). The motion to dismiss Count 17 is therefore **DENIED** as to DDC, except as to any theory of intentional misrepresentation, for which it is **GRANTED**.

vii. California Medical Information Act

1. Delta Dental (Count 14)

Plaintiffs allege that Delta Dental, Maximus, and Welltok have violated the Confidentiality of Medical Information Act ("CMIA"), a healthcare privacy statute prohibiting any "provider of health care, health care service plan, . . . or contractor" from releasing an individual's medical information except as specifically allowed. Cal. Civ. Code § 56.101. A "provider of healthcare" includes an entity that "offers software or hardware to consumers . . . designed to maintain medical information." Id. § 56.06(b).

First, Delta Dental argues that the Court must dismiss all CMIA claims as to non-California residents because only California plaintiffs may bring a CMIA claim. [Delta Dental Mem. at 66]. Of the 14 Delta Dental Bellwether Plaintiffs, only two are California residents. [Id.]. The Court agrees. Collins v. Conifer Value-Based Care, No. 24-cv-02265, 2025 WL 1140788, at *8 (C.D. Cal. Feb. 28, 2025) (stating that only a California plaintiff can bring a CMIA claim).

That leaves Plaintiffs Duarte and Moralez. Delta Dental argues that these Plaintiffs have insufficiently alleged that their medical information was viewed, as is required by the statute. [Delta Dental Mem. at 67]. The Court agrees. Sutter Health v. Super. Ct., 227 Cal. App. 4th 1546, 1556–57 (2014) ("[I]n order to violate the [Confidentiality Act], a provider of health care must make an unauthorized, unexcused disclosure of privileged medical information." (second alteration in original) (emphasis added) (citation omitted)). Plaintiffs only allege that "Private Information" was viewed, see, e.g., [CAC ¶ 2766], and make no allegations about medical information in particular. Thus, Delta Dental's motion to dismiss Count 14 is **GRANTED**.

The only parties involved in the CMIA claim with regard to Maximus are Plaintiff McCaskell against MFSI and here, Plaintiff actually alleges that "medical information" was exposed in the breach. See, e.g., [CAC ¶ 3169]. Maximus makes several arguments for dismissal. First, they argue that the mere occurrence of a data breach is insufficient to establish a failure to implement adequate security measures. [Maximus Mem. at 65]. For reasons similar to the Court's reasoning under the negligence claims, see supra, the Court rejects this argument.

Second, MFSI argues that it did not affirmatively disclose Plaintiff McCaskell's information, and therefore a CMIA claim cannot be maintained because "[t]he CMIA penalizes only intentional disclosures, not data breaches by third-party actors." [Maximus Mem. at 67]. Notably, Plaintiff McCaskell brings the claim under two different provisions of the CMIA, sections 56.10 and 56.101. It appears that the bulk of California courts require an affirmative disclosure under section 56.10 (under which a party can recover under section 56.35) but not under section 56.101 (under which a party can recover under section 56.36). See, e.g., In re Ambry Genetics Data Breach Litig., 567 F. Supp. 3d 1130, 1148 (C.D. Cal. 2021) with Sutter Health, 227 Cal. App. 4th at 1556.

Section 56.101 only requires an allegation that the information was actually viewed by an unauthorized person; it does not require affirmative disclosures. Sutter Health, 227 Cal. App. 4th at 1556. And Plaintiff has met that burden here. See [CAC ¶¶ 3165, 3168]. Thus, MFSI's motion to dismiss Count 10 is **DENIED**.

Finally, Bellwether Plaintiffs Copans and Meyer assert CMIA claims against Welltok and Sutter Health. [Compl. ¶ 3633]. Defendants first argue that Welltok is not a healthcare provider, and therefore claims under the CMIA cannot be sustained. [Welltok Mem. at 57]. Although the case law is mixed on the issue, compare In re Blackbaud, Inc., Customer Data Breach Litig., No. 20-mn-02972, 2021 WL 3568394, at *8 (D.S.C. Aug. 12, 2021) (agreeing with plaintiffs that Blackbaud is a healthcare provider because it offered services for purposes related to medical information), with In re Accellion, Inc. Data Breach Litig., 713 F. Supp. 3d 623, 644 (N.D. Cal. 2024), reconsideration denied, No. 21-CV-01155, 2024 WL 4592367 (N.D. Cal. Oct. 28, 2024) (finding plaintiffs failed to allege that Accellion was a healthcare provider within the meaning of § 56.10), the Court agrees with Welltok. As Plaintiffs note, "CMIA's definition of a provider of healthcare therefore also includes in relevant part: '[a]ny business that offers software or hardware to consumers . . . for the diagnosis, treatment, or management of a medical condition of the individual.'" [Welltok Opp. at 49 (emphasis added) (quoting Cal. Civ. Code § 56.06(b))]. To read the term "consumers" to cover the healthcare entities, such as the VCEs that actually use Welltok's service, would be "a tenuous interpretation that threatens to read the 'consumers' language out of the statute." Accellion, 713 F. Supp. 3d at 644. Therefore, the motion to dismiss Count 8 against Welltok is **GRANTED**.

On the other hand, the only argument that Sutter Health makes is reminiscent of MFSI's challenge to the adequacy of the CAC's allegations that medical information was viewed. The

Plaintiffs allege both that "they received notice letters from Welltok informing them that their names, dates of birth, health insurance information, provider names, treatment cost information, and treatment information or diagnoses were compromised" and "that following the Data Breach, CL0P released their Private Information onto the dark web, where it has subsequently been downloaded, cleaned, and reposted on the dark web by other cybercriminals," [Welltok Opp. at 51–52 (citing CAC ¶¶ 265, 285, 1199–1211, 3636)]. This is sufficient. The motion to dismiss count 8 against Sutter Health is **DENIED**.

viii. Connecticut Unfair and Deceptive Trade Practice Act

Plaintiff Boginski alleges that Delta Dental violated the Connecticut Unfair and Deceptive Trade Practices Act ("CUTPA"). To sustain a CUTPA claim a plaintiff must establish that "(1) the defendant was acting in trade or commerce; (2) that the defendant engaged in unfair or deceptive acts; and (3) that such unfair or deceptive acts caused the plaintiff to suffer an ascertainable loss." Edwards v. McMillen Cap., LLC, 574 F. Supp. 3d 52, 70 (D. Conn. 2021), aff'd, No. 21-1024-cv, 2022 WL 16984534 (2d Cir. Nov. 17, 2022).

Delta Dental argues for dismissal on two grounds: first that Boginski's unfair practice claims are preempted by the Connecticut Unfair Insurance Practices Act ("CUIPA"), and second that Boginski improperly predicates her CUTPA claim on alleged violations of other statutes that do not authorize a private right of action. [Delta Dental Mem. at 77–78].

With regards to preemption, Delta Dental's argument rests, in the first instance, on the proposition that CUIPA preempts claims arising from "general insurance practices." As the Connecticut Supreme Court has explained:

> Because CUIPA provides the exclusive and comprehensive source of public policy with respect to general insurance practices, we conclude that, unless an insurance related practice violates CUIPA

> or, arguably, some other statute regulating a specific type of insurance related conduct, it cannot be found to violate any public policy and, therefore, it cannot be found to violate CUTPA.

State v. Acordia, Inc., 73 A.3d 711, 732 (Conn. 2013).

Although Boginski concedes that CUIPA governs CUTPA claims pertaining to the "business of insurance," Conn. Gen. Stat. § 38a-816, she contends that the data security practices at issue here are not "insurance related practice[s]" and thus fall outside the preemptive scope of CUIPA. Acordia, 73 A.3d at 732. She argues that the CUIPA's provisions are aimed at "insurance-specific practices and do not purport to occupy the field of all possible conduct that an insurer may undertake." [Delta Dental Opp. at 57]. She notes that the statute "does not reference an insurer's conduct related to data breaches or employment discrimination." [Id.] Thus, while CUIPA provides the correct avenue for challenging an insurance company's claim appraisal practices, see Artie's Auto Body, Inc. v. Hartford Fire Ins. Co., 119 A.3d 1139, 1151 (Conn. 2015), or claim settlement practices, see New Eng. Sys., Inc. v. Citizens Ins. Co. of Am., No. 20-cv-01743, 2021 WL 1978691, at *3–4 (D. Conn. May 17, 2021), Boginski maintains that she can sue Delta Dental under CUTPA for its cybersecurity practices, because they have nothing to do with the business of insurance. [Delta Dental Opp. at 58].

The Court agrees with Boginski. The Connecticut Supreme Court has never held that CUIPA short-circuits CUTPA claims against insurance companies where the nature of the claims is, as here, unconnected to the defendant's status as an insurer. The ruling in Acordia does not sweep as broadly as Delta Dental would have it as there is nothing in the case law to suggest CUIPA preempts all manner of claims against insurance companies. The "sole question" before the court was "whether conduct by an insurance company that is related to its insurance business

can be found to violate CUTPA when it does not violate CUIPA."[26] Acordia, 73 A.3d at 727 n.7. That focus on "conduct . . . related to [an insurer's] insurance business" supposes, as Boginski urges, that insurers are governed by the standards of CUTPA liability with respect to aspects of their business that are not intimately involved with insurance. [Id.]. This conclusion has been embraced by lower courts in Connecticut which have explained that "an insurance company could engage in conduct which would violate CUTPA and not violate CUIPA and still be liable under CUTPA if the conduct was not, as it is here, related to its insurance business." State v. Acordia, Inc., No. X10UWYCV074020455S, 2010 WL 1752167, at *8 n.3 (Conn. Super. Ct. Apr. 19, 2010), rev'd on other grounds 73 A.3d at 711.

Delta Dental also argues that Boginski improperly "predicate[s] her CUTPA claim on alleged violations" of other statutes, including the Connecticut Data Breach Notification Act, the Federal Trade Commission Act ("FTC Act"), HIPAA, and the HITECH Act, that do not "authorize a private of [sic] right of action." [Delta Dental Mem. at 56]. Boginski responds that CUTPA prohibits practices that "offend[] public policy as it has been established by statutes, the common law, or otherwise," Glazer v. Dress Barn, Inc., 873 A.2d 929, 959 (Conn. 2005), and that she references these statutes as embodying such policy.

Boginski's citation to the FTC Act is proper. In interpreting CUTPA, as with its Massachusetts analog, courts "shall be guided by interpretations given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the [FTC] Act." Conn. Gen. Stat. § 42-

[26] The Court has revisited the question of when an insurance-related regulation other than CUIPA can supply the basis for a CUTPA claim at least twice. See Artie's Auto Body, 119 A.3d at 1151–1153 (Conn. 2015) (holding that insurance regulation requiring appraisers to evaluate damaged property impartially could not supply CUTPA claim to challenge insurer's practice of using hourly labor rates negotiated with auto body shops rather than purported fair-market rates); NEMS, PLLC v. Harv. Pilgrim Health Care of Connecticut, Inc., 325 A.3d 196, 201 (same, regarding surprise-billing statute).

110b(b); accord In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig., 613 F. Supp. 3d 1284, 1305 (S.D. Cal. 2020) (considering FTC Act while denying dismissal of CUTPA data breach claim). It is well-established "that Section 5 of the FTC Act was designed to protect the consumer whose data was compromised by the negligent actions of a defendant," as fits the allegations here. In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., No. 19-md-02879, 2020 WL 6290670, at *10 (D. Md. Oct. 27, 2020).

On the other hand, Delta Dental is on stronger footing with respect to the Connecticut Data Breach Notification law. MDL courts have dismissed CUTPA claims premised on violations of that statute, on the theory that it is subject to enforcement only by the state attorney general. See, e.g., Target, 66 F. Supp. 3d at 1168; In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1340 (N.D. Ga. 2019). Boginski appears to concede that an individual plaintiff cannot enforce a violation of the Connecticut Data Breach Notification Act through CUTPA for that reason. [Delta Dental Opp. at 60]. She clarifies, however, that she only invokes the data-breach statute as "reflect[ing] Connecticut's policy of protecting individuals' personal information," whereas in Target, the parties sought to "enforce the data breach statute directly." [Id.]. This slices it a bit too thin. Target made it a point to identify "states that explicitly allow enforcement of the[ir] data-breach notice statute through the[ir] consumer protection statute," and did not include Connecticut among them. 66 F. Supp. 3d at 1167. The Court will dismiss the CUTPA claim to the extent it is premised on violations of the data-breach statute.

That leaves HIPAA and the HITECH Act. As to the latter, Delta Dental offers no authority for the proposition that the requirements of HITECH Act cannot supply a basis for inferring relevant public policy under CUTPA. [Delta Dental Mem. at 78]. HIPAA presents a

closer call. The only state-court decision on point is a 2006 trial court dismissal of a CUTPA claim premised on a hospital's disclosure of patient information in alleged violation of HIPAA. Fisher v. Yale Univ., No. X10NNHCV044003207S, 2006 WL 1075035, at *4–5 (Conn. Super. Ct. Apr. 3, 2006). Although Fisher has not been expressly overturned, the Connecticut Supreme Court has cast significant doubt on its reasoning. See Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 49 (Conn. 2014) (holding that common-law action premised on HIPAA violation "is not preempted . . . and, further, that the HIPAA regulations may well inform the applicable standard of care in certain circumstances"); see also id. at 38 & n.8 (explaining that the lower court erroneously relied on the reasoning in Fisher). The Court thus declines to dismiss Boginski's CUPTA claim to the extent her theory of unfairness encompasses HIPAA's privacy requirements.

The motion to dismiss the CUTPA claim is **GRANTED** to the extent it is premised on the Connecticut Data Breach Notification law and otherwise **DENIED**.

ix. Georgia Uniform Deceptive Trade Practices Act

In Count 19 alleged against Delta Dental, Plaintiffs Doris Cadet and Taneisha Robertson seek injunctive relief under the Georgia Uniform Deceptive Trade Practices Act ("GUDTPA"). Delta Dental argues that the claim must be dismissed in light of the Court's ruling on standing, which dismissed certain claims for injunctive relief. [Delta Dental Mem. at 65–66]; see also [ECF No. 1304 at 6 n.3]. As explained supra, Plaintiffs are correct that the ruling on standing was based on the premise that injunctive relief cannot protect Plaintiffs from future misuse of data that Cl0p has already stolen. [Delta Dental Opp. at 44–45]. That is different from the request for injunctive relief that Plaintiffs assert here, which addresses the risk of a separate, future data breach due to ongoing deficiencies in Delta Dental's cybersecurity program. Plaintiffs specifically allege that Delta Dental has been subject to repeated data breaches, [CAC

¶ 2538 & n.720], that Delta Dental has yet to improve its cybersecurity program, [id. ¶¶ 2555, 2741], and that Delta Dental continues to possess Plaintiffs' data, [id. ¶ 2564]. In light of these allegations, the Court declines to foreclose such relief at this stage. See Arby's. Rest. Grp., 2018 WL 2128441, at *15 ("Arby's arguments are premature at this stage. Plaintiffs made specific allegations that they would be harmed without declaratory relief because Arby's has not taken steps to address their allegedly inadequate security system. This is enough to survive a motion to dismiss."). The motion to dismiss the GUDTPA claim is **DENIED**.

x. Illinois Private Information Protection Act and Illinois Consumer Fraud Act

To recover under the Illinois Consumer Fraud Act, a plaintiff must "show they suffered 'actual damages' due to the defendant's violation." Ramirez v. LexisNexis Risk Sols., 729 F. Supp. 3d 838, 849 (N.D. Ill. 2024) (citation omitted). "The actual damages element . . . requires that the plaintiff suffer 'actual pecuniary loss.'" Id. at 850 (quoting Kim v. Carter's Inc., 598 F.3d 362, 365 (7th Cir. 2010)). A pecuniary loss must be "real and measurable," and once the plaintiff shows that they have "suffered an economic loss, noneconomic injuries are compensable." Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 830 (7th Cir. 2018); accord Yepez v. Specialized Loan Servicing, LLC, No. 18-C-07422, 2019 WL 2644255, at *4 (N.D. Ill. June 27, 2019) ("Illinois requires provable economic loss before a party is entitled to aggravation, inconvenience, and emotional loss.").

PBI and TIAA aver that Uhrich "only alleges 'an increase in spam/phishing calls,' 'time spent . . . monitoring accounts,' and the risk of future harm," [PBI Mem. at 77 (quoting CAC ¶¶ 910, 916)]. These do not assert "a 'real and measurable' out-of pocket loss." In re SuperValu Customer Data Sec. Breach Litig., 925 F.3d 955, 964 (8th Cir. 2019). Welltok similarly argues that Rehm's allegations of "fraud and identity theft; time and expenses related to monitoring their

financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information" fall short under ICFA, [Welltok Mem. at 69–70 (quoting CAC ¶ 3718)], and Rehm offers no citation to support a different reading. The Court agrees that, like Uhrich's injury allegations, these are inadequate.

Maximus contends that Plotke has not alleged a pecuniary loss. [Maximus Mem. at 78–79]. In particular, Maximus observes that although Plotke claims charges were made on a credit card fraudulently opened in his name, he admits that he "successfully dispute[d]" the opening of the account, [CAC ¶ 161], thus disproving the idea of a pecuniary loss. But Maximus overlooks that Plotke also alleges that he "incurred out-of-pocket expenses" in the form of "postage" in order to mitigate any loss. [CAC ¶ 161]. Maximus gives no reason why those charges are inadequate,[27] [Maximus Mem. at 78–79], and its own cases explain that although "actual damage" must be "real and measurable," the ICFA "does not require more," Dieffenbach, 887 F.3d at 829–30 (holding monthly $17 charge satisfied ICFA actual damages requirement). The Court concludes that, if only by the skin of his teeth, Plotke has met the ICFA damages requirement.

Maximus maintains that Plotke's ICFA claim is also doomed because he failed to plead that the allegedly deceptive statements caused his injuries. [Maximus Mem. at 71–72]. Plaintiffs respond that Maximus is effectively asking the Court to require that Plotke plead

[27] The Court's own review of relevant law notes that one Illinois case held that "postage . . . expenditures" are not "recoverable under the ICFA." Yepez, 2019 WL 2644255, at *4. Yepez, however, cited precedent discussing mailing expenses in the context of obtaining legal representation, which were considered as part of legal expenses, as opposed to actual damages. Id. Nothing in the CAC suggests Plotke's postage expenses related to legal services.

"actual reliance," which is "not require[d]" under the statute. Siegel v. Levy Org. Dev. Co., 607 N.E.2d 194, 198 (Ill. 1992).

While reliance, per se, is not required under the ICFA, causation is an essential element of a viable claim. "[A]s in any other tort, to sustain a cause of action under the Consumer Fraud Act, the plaintiffs must further allege that damages were proximately caused" by the defendant's actions. Adler v. William Blair & Co., 648 N.E.2d 226, 234 (Ill. App. Ct. 1995). The obligation to plead proximate cause stems from the statutory obligation to "prove that actual damages were suffered 'as a result' of the deceptive act." De Bouse v. Bayer AG, 922 N.E.2d 309, 313 (Ill. 2009). Maximus's position is that, in an action based on an alleged misrepresentation or omission, a plaintiff must actually be deceived by a statement or omission for liability to attach under the ICFA and IUDTPA. [Maximus Mem. at 71 n. 29]. On this logic, "[i]f there has been no communication with the plaintiff, there have been no statements and no omissions." Guajardo v. Skechers USA, Inc., No. 19-cv-04104, 2021 WL 4302532, at *3 (C.D. Ill. Sept. 21, 2021) (quoting De Bouse, 922 N.E.2d at 316).

While the text of the ICFA does not expressly include "actual reliance" as an element, what emerges from the cases interpreting state law is that an ICFA plaintiff "must prove that 'each and every consumer who seeks redress actually saw and was deceived by the statements in question'" in order to satisfy proximate cause. De Bouse, 922 N.E.2d at 315 (quoting Barbara's Sales, Inc. v. Intel Corp., 879 N.E.2d 910, 927 (Ill. 2007)). Plotke does not have an answer to this point and the Court finds that he has failed to state a claim that any deceptive statements by Maximus were the proximate cause of his injuries.

That leaves the PIPA claims. At the outset, the Court agrees with Defendants that PIPA does not by itself create an independent private right of action, notwithstanding some language in

decisions that Plaintiffs cite. See [Maximus Mem. at 62]. Contra, e.g., Fox v. Iowa Health Sys., 399 F. Supp. 3d 780, 800 (W.D. Wisc. 2019) ("[T]he Illinois data breach statute clearly creates a private right of action." (citation omitted)). The more persuasive view is that a violation of the PIPA is a per se "unlawful practice" under ICFA, which "allows consumers to bring private actions when damaged by an unlawful practice." Id.

In any event, even Plaintiffs' cases make clear that they "must allege actual damages to bring a claim under the Illinois . . . Consumer Fraud Act," so failure "to allege any damages that were caused by the timing of the notifications" is fatal to a PIPA claim. Fox, 399 F. Supp. 3d at 801. Rehm and Uhrich's PIPA claims therefore fail for the same pleading deficiencies as their ICFA-deception claims. The only injuries Uhrich attributes to the allegedly delayed notice relate to emotional distress, [CAC ¶ 912], which is not a pecuniary loss. Rehm does not attribute any independent harm to the breach, [id. ¶¶ 315–16], and so has failed to "allege any damages," cognizable under ICFA or not, "that were caused by the timing of the notifications." Fox, 399 F. Supp. 3d at 801. Thus, the motions to dismiss all three PIPA claims are **GRANTED**. Plotke's claim, however, does not suffer from the same deficiencies as his ICFA claim, because the PIPA allegations do not sound in fraud. Therefore, the motion to dismiss Plotke's ICFA claim is **DENIED** insofar as it is premised on a violation of PIPA.

xi. Illinois Uniform Deceptive Trade Practices Act

The Illinois Unfair and Deceptive Trade Practices Act ("IUDTPA") permits a "person likely to be damaged by a deceptive trade practice" to obtain "injunctive relief" against the offender. 815 Ill. Comp. Stat. 510/3; see also Darne v. Ford Motor Co., No. 13 C 03594, 2015 WL 9259455, at *12 (N.D. Ill. Dec. 18, 2015) ("[IUDTPA] 'provides injunctive relief for a plaintiff who can demonstrate that a defendant engaged in any of the 12 enumerated types of

conduct' listed in 815 ILCS 510/2(a)." (quoting Int'l Star Registry of Ill. v. ABC Radio Network, Inc., 451 F. Supp. 2d 982, 990 (N.D. Ill. 2006))).

PBI argues that Uhrich's claims for injunctive relief under IUDTPA must be dismissed for the same reasons discussed in this Court's decision on standing, namely, that the injunctive relief requested at that stage would not have redressed the risk of future harm associated with data that Cl0p had already accessed. [PBI Mem. at 69]. For the reasons discussed supra, the Court rejects this argument. The motion to dismiss is **DENIED** as to Count 18 against PBI.

OSF makes a similar argument with regard to Rehm's claims, and adds two additional contentions: (1) Rehm does not allege that the incident occurred in Illinois, and (2) the IDTPA claims sound in fraud and do not meet the 9(b) standard. [Welltok Mem. at 72–73].

"Courts weigh four factors in determining whether a transaction occurred primarily and substantially in Illinois: (1) the plaintiff's residence, (2) where the misrepresentation was made, (3) where the damage to the plaintiff occurred, and (4) whether the plaintiff communicated with the defendant in Illinois." LastPass, 742 F. Supp. 3d at 130 (quoting IPOX Schuster LLC v. Nikko Asset Mgmt. Co., LTD, 191 F. Supp. 3d 790, 808 (N.D. Ill. 2016)). Given that Rehm alleges that he lives in Illinois and the damages were felt there, and that OSF is also located in Illinois, the allegations are sufficient to survive a motion to dismiss. [Welltok Opp. at 63 (citing CAC ¶¶ 304, 946, 3312).

That leaves the 9(b) argument. The Court agrees that Rule 9(b) applies. CardioNet, Inc. v. LifeWatch Corp., No. 07 C 6625, 2008 WL 567031, at *2 (N.D. Ill. Feb. 27, 2008) ("IUDTPA and ICFA claims sounding in fraud must also meet the pleading requirements of Rule 9(b)."). This requires alleging specifically "the identity of the person making the misrepresentation, the

time, place, and content of the misrepresentation, and the method by which the misrepresentation was communicated." Id. at *3.

The CAC alleges that OSF's Patient Privacy & Rights promises "that OSF 'work[s] very hard to make sure the health information of our patients is properly protected.'" [Welltok Opp. at 60 (quoting CAC ¶ 3345) (emphasis in original)]. But no reasonable consumer would have interpreted such statements as a guarantee that OSF's systems would be invulnerable or that there would be no circumstances under which OSF's security systems would fail. Thus, Welltok's motion to dismiss Count 15 is **GRANTED**.

xii. Michigan Consumer Protection Act and Michigan Identity Theft Protection Act

In Counts 17 and 18 against Welltok and Corewell, Plaintiffs Williams and Weaver allege violations of the Michigan Identity Theft Protection Act ("MITPA") and the Michigan Consumer Protection Act ("MCPA"). MITPA requires businesses affected by data breaches to give notice to affected Michigan residents "without unreasonable delay." Mich. Comp. Laws § 445.72(1), (4). Welltok and Corwell argue that this claim should be dismissed because it does not afford a private cause of action. [Welltok Mem. at 77–78]. Plaintiffs apparently concede that they lack a statutory cause of action but explain that "consumers may bring a civil action to enforce [MITPA] through Michigan's consumer protection statute." [Welltok Opp. at 65–66 (quoting Lurry v. PharMerica Corp., No. 23-CV-00297, 2024 WL 2965642, at *9 (W.D. Ky. June 12, 2024))]. Even though MITPA does not afford a private right of action, Welltok and Corewell do not dispute that Williams and Weaver can pursue a MITPA violation as part of their MCPA claim, and Welltok raises no other substantive defect in Plaintiffs' claim under MITPA. See [Welltok Mem. at 78]. Therefore, the motion to dismiss Count 17 is **GRANTED** insofar as it purports to

state an independent cause of action under MITPA. Plaintiffs may, however, pursue their MITPA theory as part of their MCPA claim.

Having concluded that Plaintiffs' MITPA theory (pursued under the MCPA) survives dismissal, the Court declines to address the sufficiency of Plaintiffs' other theories at this time. To the extent Corewell asserts that it cannot be held liable under the MCPA because data security is only an incidental aspect of the medical services, [Welltok Mem. at 79], this is not something the Court can decide at the pleading stage. The gravamen of the data-collection allegations against Corewell is that they collected patient information "in connection with healthcare services" and used that information, at least in part, to enhance quality of care—including by contracting with Welltok "to connect . . . their [patients] with personalized health improvement resources." [CAC ¶¶ 3300, 3313]. While there may be challenges in developing a factual record to support such allegations, the allegations here are a far cry from the facts of the non-binding Michigan authority Corewell cites. [Welltok Mem. at 79 (citing MacLean v. RMA Physicians, No. 182666, 1996 WL 33348549, at *1 (Mich. Ct. App. Nov. 1, 1996) (per curiam))]. In MacLean, an unpublished per curiam decision,[28] the Michigan Court of Appeals held that a doctor was not engaged in "trade or commerce" under the MCPA when "copying patient records" because "the physician is not in the business of providing such a service." 1996 WL 33348549, at *1 (dismissing MCPA claim predicated on physicians' "refusal to supply plaintiff with plaintiff's father's medical record"). The allegations of the CAC, by contrast, plausibly

[28] Under Michigan law, unpublished appellate decisions are "not precedentially binding" and should only be cited for their persuasive value. Mich. Ct. R. 7.215(C)(1). In addition to finding MacLean factually inapposite based on the allegations in the Complaint, the Court is skeptical of the case's persuasive value, given that its interpretation of the term "trade or commerce" under the MCPA did not rely on ordinary canons of construction, cited no case law, and has never been cited or discussed in a ruling by any other court, in Michigan or elsewhere.

allege that Corewell's collection of patient data was more immediately entwined with its provision of medical services than the copying at issue in MacLean. The motion to dismiss Count 18 against Welltok and Corewell is **DENIED**.

xiii. Minnesota Consumer Fraud Act and Minnesota Uniform Deceptive Trade Practices Act (PBI Counts 9 and 10)

The Minnesota Consumer Fraud Act prohibits "any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice with the intent that others rely thereon in connection with the sale of any merchandise." Graphic Commc'ns Local 1B Health & Welfare Fund "A" v. CVS Caremark Corp., 850 N.W.2d 682, 694 (Minn. 2014). For a private plaintiff to recover damages under the Minnesota CFA, "the plaintiff must plead and prove a causal relationship between the alleged injury and the wrongful conduct that violates the statute." Id. at 693. The statute, moreover, "does not apply to all allegations of fraud, but only to those where there is a nexus between the alleged fraud and the sale of merchandise," which includes "services." Mekhail v. N. Mem'l Health Care, 726 F. Supp. 3d 916, 928–29 (D. Minn. 2024) (first quoting Grady v. Progressive Direct Ins. Co., 643 F. Supp. 3d 929, 935 (D. Minn. 2022); and then quoting Minn. Stat. § 325F.68, Subd. 2); accord Banbury v. Omnitrition Int'l, Inc., 533 N.W.2d 876, 882 (Minn. Ct. App. 1995).

The PBI Bellwether Defendants raise a variety of arguments as to why Plaintiffs MCPA claim should be dismissed, including a failure to plead facts supporting statutory standing, causation, and intent. The Court focuses only on the causation challenge. Defendants urge that the Minnesota Plaintiffs must "plead facts to show that the supposed misrepresentations about which they complain[] caused their harm," [PBI Mem. at 64 (emphasis in original)], which includes pleading "a connection between the type of representation" and the "insurance and financial services" that Defendants "actually sold," [id. at 66 n.39].

Plaintiffs argue that it is enough to allege that as a "direct and proximate result of . . . Defendants' fraudulent, misleading, and deceptive practices, [Plaintiffs] have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages." [PBI Opp. at 61 (alterations in original) (quoting CAC ¶ 2185, 2195)]. Plaintiffs point to the general pleading standards of Rule 8, which they suggest provides the standard for pleading causation on a CFA claim, and contend that there is "[n]o . . . requirement" under the MCFA to plead more. [Id.]

But even under Rule 8's ordinary pleading standards, a mere conclusory allegation is not enough. Minnesota decisions make clear that Plaintiffs "must plead and prove a causal relationship between the alleged injury and the wrongful conduct that violates the statute," Graphic Commc'ns, 850 N.W.2d at 693. Plaintiffs fail, moreover, to account for the cases cited by the PBI Bellwether Defendants, which require a "nexus between the alleged fraud" and the "services" they sold to the Plaintiffs. Mekhail, 726 F. Supp. 3d at 928–29.

Mekhail, in particular, appears to be directly on point. In that case, a defendant healthcare provider sought dismissal of a CFA claim that alleged that the provider had misrepresented its privacy policies in light of its use of behavioral tracking technology that shared certain health data with Meta, the parent company of Facebook and Instagram. Mekhail, 726 F. Supp. 3d at 923. The defendant argued "a lack of connection between the misrepresentations alleged . . . and the sale of any merchandise" within the meaning of the statute. Id. at 929. The court agreed, reasoning that although the statutory definition of "merchandise" covered "services" (and the court assumed "services" included "medical services"), there was no allegation "that there was a misrepresentation made by [the defendant] in connection with its provision of any medical services." Id. Rather, the Mekhail court found,

the plaintiff had "allege[d] a misrepresentation related to data privacy, but [the defendant] [was] not in the business of providing data privacy services," so the allegation did not satisfy the causal nexus requirement. Id.

Nearly identical reasoning requires dismissal here. As in Mekhail, the CAC alleges that the "PBI Bellwether Defendants' goods, services, commodities, and intangibles are 'merchandise' as defined by Minn. Stat. § 325F.68(2)." [CAC ¶ 2179]; cf. 726 F. Supp. 3d at 929 ("What the FAC alleges is that '[t]he medical services that Defendant markets, provides, offers, and/or sells are considered merchandise' under the statutory definition." (alteration in original)). The CAC, however, does not allege that any of the PBI Bellwether Defendants are "in the business of providing data privacy services." Mekhail, 726 F. Supp. 3d at 929. To the contrary, the CAC describes the PBI Bellwether Defendants as providing "life insurance" or "financial products" or as service providers to the life insurance industry. See [CAC ¶¶ 927–34]. The Mekhail court concluded that "[t]he critical issue is not . . . whether [an allegedly fraudulent] sale involved aspects that can be viewed as constituting 'merchandise,' but rather whether there is a 'nexus' between the alleged misrepresentations and that 'merchandise.'" Mekhail, 726 F. Supp. 3d at 929 (quoting Moua v. Jani-King of Minn., Inc., 613 F. Supp. 2d 1103, 1113 (D. Minn. 2009)). Viewed through this lens, the allegations here are inadequate to state a claim under the MCFA for either affirmative misrepresentations or deceptive omissions.[29]

[29] The Supreme Court of Minnesota has also explained that "an omission-based consumer fraud claim is actionable under the CFA when special circumstances exist that trigger a legal or equitable duty to disclose the omitted facts," Graphic Commc'ns, 850 N.W.2d at 695, and Plaintiffs' omission-based allegations would fail under that standard because they have identified no basis in Minnesota law for finding such a duty to disclose the alleged deficiencies in Defendants' cybersecurity procedure.

As to the MUDTPA claim, Defendants argue that the claim must be dismissed in light of the Court's standing ruling, which dismissed certain claims for injunctive relief. [PBI Mem. at 69]; see also [ECF No. 1304 at 6 n.3]. For the reasons stated supra, the Court disagrees. The motion to dismiss the MUDTPA claim is **DENIED**.

xiv. Nebraska Consumer Protection Act

In Count 19 against Welltok and CHI, Plaintiff George asserts a violation of the Nebraska Consumer Protection Act ("NCPA"). The NCPA "provides that unfair or deceptive acts or practices in the conduct of any trade or commerce that have an impact on the public interest by either directly or indirectly affecting the people of the State of Nebraska, shall be unlawful." Weisenberger v. Ameritas Mut. Holding Co., 597 F. Supp. 3d 1351,1368 (D. Neb. 2022). George specifically premises his NCPA claim on a violation of the Nebraska Data Protection Act ("NDPA"), which provides that "a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska shall implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information . . . and the resources available to, the business and its operations." Neb. Rev. Stat. § 87-808(1). Violations of the NDPA may be enforced by private plaintiffs through the NCPA. Id. § 87-806(2).

Welltok and CHI contend that George has "not allege[d] facts showing how Welltok or CHI violated the NDPA," as they "are multiple steps removed from a zero-day incident that they could not have possibly prevented." [Welltok Mem. at 83]. Plaintiff responds that a defendant may be liable under the NDPA if the defendant fails to "implement and maintain reasonable security procedures and practices." Neb. Rev. Stat. § 87-808(1). This seems adequately covered by the CAC's allegation that Welltok failed to properly safeguard its MOVEit environment and

that CHI lacked adequate vendor vetting. See [CAC ¶¶ 3364–67, 3382–88, 3453–65]. Thus, Plaintiffs have the better of this argument.

Welltok and CHI also argue that George has not alleged damages recoverable under the NCPA. Defendants contend that the NCPA requires a plaintiff to plead "actual damages," [Welltok Mem. at 82 (quoting Neb. Rev. Stat. § 59-1609)], meaning that they must plead an out-of-pocket loss. George's alleged damages, according to Welltok, are "derivative and remote," which is insufficient under that standard. See [id.]. Although there is no allegation that George has suffered a direct financial loss, the plain text of the NCPA's damages provision and Defendants' own cases do not require such an allegation. On the contrary, the statute allows "actual damages sustained" or an award of damages "not susceptible [to] measurement by ordinary pecuniary standards" up to $1,000. Neb. Rev. Stat. § 59-1609. Indeed, Nebraska courts have awarded damages under materially similar circumstances:

> Although Pauly has failed to sufficiently prove the existence of any actual damages in this case, the NCPA allows courts the discretion to award damages in "an amount which bears a reasonable relation to the actual damages which have been sustained and which damages are not susceptible of measurement by ordinary pecuniary standards[.]"

Pauly v. Oliver Wright & Assocs., 21-cv-156, 2023 WL 6046318, at *4 (D. Neb. Jan. 6, 2023) (alteration in original) (quoting Neb. Rev. Stat. § 59-1609). The Court in that case "exercise[d] its discretion" and awarded $1,000 for "'distress' and 'inconvenience'" as a result of illegal debt collection practices, even without any showing of actual damages. Id. Here, George's allegations rise at least to this standard. [CAC ¶¶ 363-64 (alleging, inter alia, loses from time and expenses spent scrutinizing financial statements, financial accounts, and credit reports for

fraudulent activity)]. That is sufficient at this stage. Welltok's motion to dismiss Count 19 is **DENIED**.

xv. Nebraska Uniform Deceptive Trade Practices Act

In Count 19 against Welltok and CHI, Plaintiff George also alleges deceptive trade practices under the Nebraska Uniform Deceptive Trade Practices Act ("NUDTPA"). To state a claim under the NUDTPA, a plaintiff must plausibly allege that the defendant made "a representation regarding the nature of goods or services and [that] the representation [was] for characteristics or benefits that the goods or services did not have." Weisenberger, 597 F. Supp. 3d at 1370. Although the statute does provide a private right of action for injunctive relief,[30] Welltok and CHI contend that George's claim fails on two grounds.

They first argue that because the NUDTPA offers private litigants only prospective relief, a plaintiff must allege she is "likely to be damaged" by the defendant's future actions. Senior Hous. Managers, LLC v. Highway 2 Dev., LLC, 552 F. Supp. 3d 866, 887 (D. Neb. 2021); see [Welltok Mem. at 30]. Some courts applying the NUDTPA have held that once a plaintiff knows about a defendant's alleged deceptive practice, she may not be able to show she is "likely" to be injured again in the future. For example, Defendants cite Reinbrecht v. Walgreen Co., where the court held the plaintiff could not demonstrate he was "likely to be damaged" by Walgreen's alleged deceptive act or practice regarding postage stamp pricing because plaintiff "now knows the truth regarding the price of postage stamps sold by Walgreens." 742 N.W.2d 243, 248 (Neb. Ct. App. 2007). Welltok and CHI contend that because "George is allegedly aware of and knows

[30] Plaintiffs have abandoned their claim for damages under the statute. [Welltok Opp. at 53 n.25].

of CHI's allegedly deceptive acts or practice, she cannot reasonably allege she is 'likely' to be damaged by the same deceptive acts or practices." [Welltok Mem. at 59 (emphasis in original)].

Defendants' argument on this score overreaches. Under their reasoning, no plaintiff would ever have a valid cause of action, since every plaintiff must know of the alleged deception before she can sue. Rather, this appears to be a fact-bound inquiry that will turn on whether a plaintiff's knowledge precludes a showing of future harm. Here, George explains that "although [she] is now aware of Defendants' deception, her Private Information remains in Defendants' inadequately secured systems," and an injunction is necessary to ensure that Defendants safeguard that information moving forward. [Welltok Opp. at 53 (citing CAC ¶¶ 3333–35]. The circumstances here are thus very different from those in Walgreens. George's knowledge about Welltok's and CHI's cybersecurity does not change the fact that the Defendants continue to possess her information, which she plausibly alleges will remain at risk of future harm absent an injunction. [CAC ¶¶ 3602–04]. At this stage, these allegations suffice to state a claim for injunctive relief.

Second, Defendants argue that injunctive relief under the NUDTPA cannot be based on a deceptive representation concerning services that were "ancillary" to defendant's primary trade. Weisenberger, 597 F. Supp. 3d at 1370. CHI contends that its primary "trade" is healthcare, not data security, so it cannot be liable under NUDPTA. [Welltok Mem. at 85].

George disputes whether Weisenberger correctly interpreted the NUDPTA. [Welltok Opp. at 70]. Even assuming it does, the allegations here are sufficient to state a claim. George alleges that CHI collected her information as part of its "healthcare services" and shared that information with Welltok to "provide patients . . . with important notices and communications" regarding those patients' healthcare. [CAC ¶ 3314]. In other words, the CAC alleges that

collecting and sharing George's data was part and parcel of CHI's core business, not an ancillary service.

The motion to dismiss the NUDTPA claim is therefore **DENIED**.

xvi. New Jersey Consumer Fraud Act

Like Progress, PBI and TIAA argue that Plaintiff Phelan's New Jersey Consumer Fraud Act ("NJCFA") claim is subject to dismissal based on the lack of any allegation of a direct consumer relationship. As the Court explained in MDL Order No. 22, recent data breach cases requiring a direct transaction between the litigants overlook state-court precedent making clear that "privity is not a condition precedent to recovery under the [NJ]CFA." Gonzalez v. Wilshire Credit Corp., 988 A.2d 567, 574 n.9 (N.J. Super. Ct. App. Div. 2010) (quoting Neveroski v. Blair, 348 A.2d 473, 479 (N.J. Super. Ct. Ap. Div. 1976)). The statute "encompass[es] the acts of remote suppliers," Perth Amboy Iron Works, Inc. v. Am. Home Assurance Co., 543 A.2d 1020, 1026 (N.J. Super. Ct. App. Div. 1988), and does not require "that the claimant have a direct contractual relationship with the seller of the product or service," Katz v. Schachter, 598 A.2d 923, 926 (N.J. Super. Ct. App. Div. 1991). Nor is the Court persuaded that the NJCFA liability is extinguished because Phelan "inherited a family member's TIAA account," [CAC ¶ 868], rather than having purchased TIAA's services or products herself. The statute applies broadly to "any person who suffers any ascertainable loss," N.J. Stat. Anns. § 56:8-19, and were that not enough, the NJCFA is "remedial legislation" that should "be construed liberally in favor of consumers," Cox v. Sears Roebuck & Co., 647 A.2d 454, 461 (N.J. 1994).

PBI and TIAA also raise lack of intent to conceal as a ground for dismissal. [PBI Mem. at 78]. Because Phelan alleges that PBI and TIAA "committed deceptive omissions in violation of the NJCFA," [CAC ¶ 2312], she must allege that they concealed information "with the intention that [she] rely upon the concealment." Arcand v. Brother Int'l Corp., 673 F. Supp. 2d

282, 297 (D.N.J. 2009) (citing Judge v. Blackfin Yacht Corp., 815 A.2d 537, 542 (N.J. Super. Ct. App. Div. 2003)); see also In re U.S. Vision Data Breach Litig., 732 F. Supp. 3d 369, 382 (D.N.J. 2024) ("To adequately plead an omission, a plaintiff must further allege that the defendant (1) knowingly concealed (2) a material fact (3) with the intention that the consumer rely upon the concealment." (quoting In re Am. Fin. Res., Inc., Data Breach Litig., No. 22-cv-01757, 2023 WL 3963804, at *10 (D.N.J. 2023))). Phelan argues that the CAC "provides detailed descriptions regarding PBI and TIAA's misrepresentations." [PBI Opp. at 73] Regardless of the truth or falsity of these alleged misrepresentations, the CAC is devoid of any plausible allegation that PBI or TIAA intentionally concealed information about alleged defects in their cybersecurity programs or that they intended that Phelan rely on such concealment. The motion to dismiss the NJCFA claim is **GRANTED**.

xvii. New York General Business Law

Several Plaintiffs allege violations of section 349 of the New York General Business Law: Gilbert and Lynda Hale against PBI and Genworth (Count 20); Plaintiffs Gonsalves and Kavanagh against Delta Dental (Count 24); and Barbara Cruciata against Maximus (Count 14).

In general, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in [New York] are . . . unlawful." N.Y. Gen. Bus. Law § 349(a). "To state a claim, a plaintiff must allege (1) that the defendant's acts were consumer oriented, (2) that the acts or practices are deceptive or misleading in a material way, and (3) that the plaintiff has been injured as a result." In re Unite Here Data Sec. Incident Litig., 740 F. Supp. 3d 364, 386 (S.D.N.Y. 2024) (citation omitted).

PBI argues that it does not engage in consumer-oriented content. [PBI Mem. at 79]. PBI and Genworth also argue that the claims falter on the second and third prong because (1) the representations and omissions identified in the CAC were not deceptive, and (2) Gilbert and

Lynda Hales have not pled that any such communications or omissions caused them to suffer injury because they do not allege that they actually saw or read any of the allegedly deceptive content. [PBI Mem. at 64–66].

Under the GBL, a plaintiff cannot state a claim if "the complaint fails to allege that the individual plaintiff . . . ever saw the allegedly deceptive representations that purportedly harmed them." Himmelstein, McConnell, Gribben, Donoghue & Joseph, LLP v. Matthew Bender & Co., 100 N.Y.S.3d 227, 229 (N.Y. App. Div. 2019), aff'd, 171 N.E.3d 1192. Thus, "[t]o establish the requisite causal connection between an alleged written misrepresentation and the resulting injury, [a] plaintiff must plausibly allege that she actually viewed the misleading statement prior to making her decision to purchase, and must set forth where, when and how she came to view it." In re GEICO Customer Data Breach Litig., No. 21-cv-02210, 2023 WL 4778646, at *17 (E.D.N.Y. July 21, 2023) (second alteration in original) (citation omitted).

PBI and Genworth assert that there is no such allegation here. [PBI Mem. at 64]. In rebuttal, Plaintiffs do not contend that they have pleaded reliance; rather their sole response is to contend that reliance is not a requirement under GBL section 349. [PBI Opp. at 73]. In a literal sense, this may be true. See Gale v. Int'l Bus. Machines Corp., 781 N.Y.S.2d 45, 46 (N.Y. App. Div. 2004) ("Reliance is not an element of a claim under General Business Law § 349."). That said, the cases make clear that "the plaintiff must show that the defendant's material deceptive act caused the injury," and reinforce the principle that PBI and Genworth assert here: namely that "[i]f the plaintiff did not see any of the[] statements, they could not have been the cause of his injury." Id. at 47; see also id. (dismissing claim on that basis, because plaintiff "failed to plead causation with sufficient specificity to withstand dismissal").

In sum, Plaintiffs' apparent concession that they have not pleaded reliance is "fatal to the[ir] claim." Geico, 2023 WL 4778646, at *17.

Additionally, the Court also agrees that the Hales have not alleged deceptive conduct under the GBL. "A defendant's actions are materially misleading when they are 'likely to mislead a reasonable consumer acting reasonably under the circumstances.'" Himmelstein, McConnell, Gribben, Donoghue & Joseph, LLP v. Matthew Bender & Co., 171 N.E.3d 1192, 1198 (N.Y. 2021) (quoting Gaidon v. Guardian Life Ins. Co. of Am., 725 N.E.2d 598, 604 (N.Y. 1999)). "A misrepresentation can come in the form of an affirmative misrepresentation or a materially deceptive omission." Yuille v. Uphold HQ Inc., 686 F. Supp. 3d 323, 344 (S.D.N.Y. 2023).

Plaintiffs point to two categories of affirmative misrepresentations allegedly made by PBI and Genworth. First, they allege PBI and Genworth made statements recognizing the importance of privacy and cybersecurity, [PBI Opp. at 24], such as the following:

- "[P]rotecting and securing the information of [PBI's] clients and [the] company is of critical importance to PBI. We recognize that all relationships with current and prospective clients are based upon integrity and trust, and we take our role as custodians of confidential information very seriously." [CAC ¶ 1841 (second alteration in original)].
- "Data security is a company imperative. PBI strives to protect personally identifiable information that [it] collect[s], maintain[s], process[es], or disclose[s], including by using appropriate administrative, physical, and technical safeguards." [Id. ¶ 1843 (alterations in original)].
- PBI is "commit[ted] to the responsible use of information and protection of individual privacy rights[]." [Id. (second alteration in original)].
- "PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment." [Id. ¶ 1844].
- "[W]orking to protect [its customers'] personal information is one of [the] promises that enables [Genworth] to help millions of policyholders secure their financial lives, families, and futures." [Id. ¶ 1859]

Second, Plaintiffs point to statements describing practices PBI and Genworth undertake toward those ends:

- PBI would "obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate." [CAC ¶ 1845].
- PBI has "the largest team of data scientists, product developers, security and IT, and subject matter experts in the industry" and "aspire[s] to protect individuals' privacy through the design of [its] products and services, by credentialing, monitoring, and auditing [its] business clients as appropriate, and through other information security safeguards." [Id. ¶ 1846 (alterations in original)].
- PBI "use[s] a variety of administrative, physical and technical security measures intended to safeguard your personal information." [Id. ¶ 1848].
- Genworth "implement[s] technical, physical, and process safeguards to maintain the confidentiality of your information." [Id. ¶ 1861].
- "Once [Genworth] receive[s] your information, we use procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. We maintain physical, electronic, and procedural protections to protect personal information in accordance with applicable standards." [Id. ¶ 1860]
- "[Genworth] require[s] that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated." [Id. ¶ 1860].

Plaintiffs also allege that PBI and Genworth made two material omissions:

- "Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII;" [CAC ¶ 2321(f)], and
- "Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII . . . ." [Id. ¶ 2321(g)].

PBI and Genworth argue these allegations boil down to no more than statements that they "would protect the privacy and confidentiality of [plaintiffs'] PII," [PBI Mem. at 66 (quoting CAC ¶ 2321(d)) (alteration in original)], and that such statements were not deceptive because they "do not constitute an unlimited guaranty that [plaintiffs'] information could not be stolen." Smahaj v. Retrieval-Masters Creditors Bureau, Inc., 131 N.Y.S.3d 817, 827–28 (N.Y. Sup. Ct. 2020). Plaintiffs suggest in response that such statements constituted "blanket representations about the adequacy of its security." [PBI Opp. at 58 (quoting Yuille, 686 F. Supp. 3d at 347)].

The Court agrees with PBI and Genworth, based primarily on the reasoning in Yuille. As the court explained in Yuille, a statement may be misleading under New York law when it is false, or when the statement, though "literally true," either is "removed from its context and the nondisclosure of its context renders the statement misleading," or it carries "two or more commonly understood meanings, one of which is deceptive." Yuille, 686 F. Supp. 3d at 345–46. The allegations of the CAC do not satisfy any of these conditions. Apart from the bare fact that the Data Breach occurred, the CAC does not allege that any of the statements they identify were false when made. The CAC does not plausibly allege that any of the measures PBI and Genworth purportedly promised would necessarily have prevented the data breach. Nor could a reasonable consumer have interpreted the foregoing statements "to provide an assurance that there would be no circumstances under which [PBI or Genworth's] security systems," or those of Progress, "would fail or that its [systems] would be invulnerable to third-party attacks." Id. at 346. Finally, Plaintiffs do not allege that PBI or Genworth "knew its security was inadequate" and failed to say so. Id. at 347. The motion to dismiss Count 20 against PBI and Genworth is **GRANTED**.

Delta Dental does not raise reliance or deception, but instead contends that Plaintiffs Gonsalves and Kavanagh's claim fails to allege that "the 'transaction in which the[y] . . . [were] deceived . . . occur[ed] in New York.'" [Delta Dental Mem. at 80 (quoting NCB, 748 F. Supp. 3d at 289)]. A claim "falls within the territorial reach" of the GBL when the plaintiff alleges "a sufficient nexus between [the plaintiff's] transactions with [the defendant] and New York." NCB, 748 F. Supp. 3d at 289 (alterations in original) (quoting MacNaughton v. Young Living Essential Oils, LC, 67 F.4th 89, 99 (2d Cir. 2023)). Plaintiffs and Delta Dental agree that courts generally look to whether "the deception occurred in New York." In re Marriott Int'l, Inc., Customer Data

Sec. Breach Litig., 440 F. Supp. 3d 447, 493 (D. Md. 2020), 493; see also In re Fortra, 749 F. Supp. 3d at 1278 ("[Section] 349's territorial requirement mandating that an act occur 'in this state' contemplates where a plaintiff was deceived." (emphasis in original)).

Gonsalves and Kavanagh thus run into the same issue Gilbert and Lynda Hales faced: they have not alleged that they ever actually saw Delta Dental's allegedly deceptive statements, let alone when or where they did so. They argue only that they "reside in New York, provided their private information to DDC from New York, received DDC's services and notice of breach in New York, and experienced harm in New York, including spending time monitoring their financial accounts." [Delta Dental Opp. at 63 (citing CAC ¶¶ 465–503)]. Such allegations, however, do not establish the critical consideration under New York law. To be deceived, they must have seen the statements, Gale, 781 N.Y.S.2d at 47, meaning that for "the deception" to have "occurred in New York," Marriott Int'l, 440 F. Supp. 3d at 493, the Plaintiffs must allege that they saw or otherwise received the statements in New York. Their failure to do so defeats their claim. The motion to dismiss Count 24 against Delta Dental is **GRANTED**.

MFSI likewise argues that the GBL claim must fail due to an insufficient nexus with New York. [Maximus Mem. at 61 (citing Goshen v. Mut. Life Ins. Co. of New York, 98 N.Y.2d 314, 324 (2002) ("the transaction in which the consumer is deceived must occur in New York."). Although the relevant Plaintiff, Cruciata, lives in New York, that bare fact is insufficient to state a claim. The motion to dismiss Count 14 against Maximus is **GRANTED**.

xviii. North Carolina Identity Theft Protection Act and North Carolina Unfair and Deceptive Trade Practices Act

In Counts 15 and 16, Plaintiff Ben Dieck alleges that Maximus violated the North Carolina Identity Theft Protection Act ("NCITPA") and the North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA"). "A plaintiff must bring a claim for a violation of the

NCITPA under the [NC]UDTPA,"[31] and to do so, must show "(1) an unfair act (2) in or affecting commerce (3) proximately causing injury." Rogers v. Keffer, Inc., 243 F. Supp. 3d 650, 662 (E.D.N.C. 2017) (quoting Reid v. Ayers, 531 S.E.2d 231, 235 (N.C. Ct. App. 2000)). North Carolina law sets a high bar for Rule 12(b)(6) dismissal of NCUDTPA claims on causation grounds. "Ordinarily, when a complaint 'adequately recites the element of causation . . . plaintiff has made a sufficient pleading of causation under Rule 12(b)(6).'" Jones v. J. Kim Hatcher Ins. Agencies Inc., 893 S.E.2d 1, 7 (N.C. Ct. App. 2023) (quoting Est. of Long ex rel. Long v. Fowler, 841 S.E.2d 290, 299 (N.C. Ct. App. 2020)), aff'd in part, rev'd in part on other grounds, 915 S.E.2d 118 (2025). Dismissal may be appropriate, however, "when it appears affirmatively from the complaint that there was no causal connection between the alleged [misconduct] and the injury." Id. (internal quotation marks and citation omitted).

Here, Plaintiffs allege that "[a]s a direct and proximate result of MSI's violations of [NCITPA], Plaintiff Dieck and North Carolina MSI Class Members suffered damages, as alleged above." [CAC ¶ 3229]. The foregoing allegations allege just one injury allegedly traceable to the delay:

> The Data Breach has caused Plaintiff Dieck anxiety, sleep disruption, stress, anger, fear for his personal financial security, and fear for what information was revealed in the Data Breach, which has been compounded by Defendants' nearly 3-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

[31] Although Plaintiff purports to assert this claim as an independent cause of action, as opposed to a claim under the NCUDTPA, Maximus does not argue for dismissal on that basis. The Court will therefore construe Count 17 as a claim under the NCUDTPA premised on a violation of NCITPA.

[CAC ¶ 71].[32] The gist of this allegation is that Dieck's emotional distress was somehow worse because he found out about the Data Breach later than he would have in a counterfactual world with quicker notification.

Dieck does not allege that the delay prevented him from "taking appropriate protective measures" sooner or that he suffered fraud "resulting from the breach before [he was] notified of it." Ambry, 567 F. Supp. 3d at 1141. Rather, his sole theory of injury is that the emotional distress he experienced after learning of the breach was compounded by the three-month lapse between the breach and the notice. [CAC ¶ 71]. The allegations of the CAC provide no factual basis for concluding that this alleged incremental increase in his emotional distress was legally caused by, or was a reasonably foreseeable consequence of, the timing of notice, as opposed to the Data Breach itself. Conceivably a delay could, in some circumstances, proximately cause an incremental emotional injury, but without allegations identifying such circumstances, Dieck's allegations fail. A plaintiff "must state a plausible, not merely a conceivable, case for relief." Ocasio-Hernandez, 640 F.3d at 12 (quoting Sepúlveda-Villarini v. Dep't of Educ., 628 F.3d 25, 29 (1st Cir. 2010) (Souter, J.)).

By definition, everyone who sues as a Data Breach victim must have learned about the breach at some point, whether sooner or later. Absent any allegation of (1) what action Dieck would have taken; (2) what separate, concrete harm Dieck would have avoided; or (3) factual allegations supporting how the emotional distress he alleges was a foreseeable consequence of the delay, a conclusory allegation that he suffered emotional distress

[32] Dieck describes his other damages, including increased risk of future identity theft, time spent on mitigation efforts, loss of the value of his PII, injury to his privacy, as being "a result of the Data Breach," and does not suggest in the CAC or in the Opposition filing that those harms were compounded by Maximus's alleged delay. [CAC ¶ 72].

following a three-month gap between breach and notice does not support a plausible inference of proximate cause.

Dieck alleges additional theories of liability under NCUDTPA, for which Maximus urges dismissal. [Maximus Mem. at 45–49]. For similar reasons as in MDL Order No. 22, these claims fail. Dieck concedes that he "ha[d] no known relationship" with Maximus or the Colorado Department of Human Services, the government entity through which Maximus obtained Dieck's information. [CAC ¶ 61]. Because Dieck acknowledges that he has no idea how his information ended up on Maximus's MOVEit interface, he cannot plausibly allege that Maximus's misrepresentations and omissions proximately caused his injuries. Cf., e.g., Fortra, 749 F. Supp. 3d at 1279 (denying a motion to dismiss NCUDTPA claim where plaintiffs alleged that defendants made misrepresentations and omissions that gave rise to a duty to disclose because plaintiffs and defendants had a direct relationship).

Maximus's motion to dismiss Counts 15 and 16 is **GRANTED**.

xix. Pennsylvania Unfair Trade Practices and Consumer Protection Law

Three Plaintiffs bring claims under the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("PUTPCPL"): Dovberg in Count 25 against Delta Dental, DiLuigi ins Count 17 against Maximus, and Checchia in Count 21 against PBI. Defendants urge a range of reasons for dismissal.

PBI and Delta Dental assert that Dovberg's and Checchia's claims fail for failure to plead justifiable reliance. [PBI Mem. at 63–64]; [Delta Dental Mem. at 82]. "To state a claim under the UTPCPL, a plaintiff must show that she 'justifiably relied on the defendant's wrongful conduct.'" In re Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 542 (M.D. Pa. 2021) (quoting Yocca v. Pittsburgh Steelers Sports, Inc., 854 A.2d 425, 438 (Pa. 2004)). The Court

agrees that Plaintiffs "fail to explicitly plead their reliance" on the Delta Dental and PBI policies and statements that they identify in the CAC. Id. (emphasis in original).

Plaintiff Dovberg asserts that he "relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect his Private Information and privacy rights," [CAC ¶ 444], and identifies an August 14, 2020 privacy statement on the Delta Dental website that offers certain assurances regarding cybersecurity, [id. ¶ 2417 & n.657]. But no allegation indicates that Dovberg actually viewed that statement, let alone that he justifiably relied on it. In his opposition, Dovberg appears to shift the focus of his PUTPCPL claim from an affirmative misrepresentation theory to an "omission" theory. [Delta Dental Opp. at 64]. This is at odds with the allegations in the CAC, which clearly state affirmative misrepresentations, alongside omissions. See, e.g., [CAC ¶ 2912(d) (alleging that Delta Dental "[m]isrepresent[ed] that they would protect the privacy and confidentiality of Plaintiff Dovberg's [PII]"). That he also alleges omissions, e.g. [id. ¶ 2912(f) (alleging Delta Dental "[o]mitt[ed] . . . the material fact that they did not properly secure [his] . . . Private Information")], alongside material misrepresentations does not excuse the requirement to plausibly allege reliance with respect to the purported affirmative misrepresentations.

As to the alleged omissions, it is true that a "plaintiff who asserts a [P]UTPCPL claim that is based on a defendant's material omission may be entitled to a reasonable inference of reliance," Cave v. Saxon Mortg. Servs., Inc., No. 11-4586, 2013 WL 460082, at *1 (E.D. Pa. Feb. 6, 2013), but only "under narrow circumstances not present" in data breaches, Rutter's, 511 F. Supp. 3d at 544 (quoting Moore v. Angie's List, Inc., 118 F. Supp. 3d 802, 817 n.8 (E.D. Pa. 2015)).

Dovberg does not seriously argue that the circumstances of this case warrant an inference of reliance. Indeed, a key feature of the cases in which the inference is warranted is that the defendant is under a "duty to speak." See, e.g., Rutter's, 511 F. Supp. 3d at 543. The Court agrees with prior cases which have found that holders of customer data, without more, do not owe a duty to disclose alleged shortcomings in their cybersecurity programs. Id. at 543–44, 544 n.12 (explaining that even if a defendant owes a "legal duty to safeguard [personal information]" it does not follow that "the duty necessarily extends to alerting customers as to the potential activities of future third-party hackers" or the defendant's potential vulnerability thereto). Delta Dental's motion is **GRANTED** as to Count 25.

Checchia's allegations fare no better. He, too, makes no claim that he viewed or otherwise received any deceptive communication from PBI or TIAA. Nor does he identify circumstances that would warrant a presumption of reliance. [PBI Opp. at 74–75]. Instead, he makes a cursory assertion that "in an analogous consolidated data breach case, the court sustained the plaintiff's [P]UTPCPL claim without analyzing any allegation of reliance," [id. at 75 (citing In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig., 614 F. Supp. 3d 1284, 1308 (S.D. Cal. 2020))]. Even the case he cites, however, does not really support his position; the Solara court expressly stated that a plaintiff must allege "justifiable reliance on that [deceptive] act." 614 F. Supp. 3d at 1308. The lack of analysis regarding reliance in that case can hardly be taken as license to ignore the issue when it has been properly raised by PBI and TIAA. Accord AMCA, 2021 WL 5937742, at *32 (dismissing "PUTPCPL claims for failure to plead reliance"). PBI and TIAA's motion is **GRANTED** as to Count 21.

Maximus contends that, among other defects, DiLuigi fails to allege an ascertainable injury, [Maximus Mem. at 79–80], or a consumer relationship with Maximus, [id. at 63–64]. The

Court agrees with Maximus as to the former justification and declines to reach the latter. "A plaintiff asserting a [P]UTPCPL claim must sufficiently allege an ascertainable loss that stems from one's justifiable reliance on the defendant's wrongful conduct." Rutter's, 511 F. Supp. 3d at 541. "To allege an ascertainable loss, the plaintiff 'must be able to point to money or property that he would have had but for the defendant's fraudulent actions,'" ordinarily by pleading "a quantifiable amount of money he lost." Id. (citation omitted). "These damages must be identifiable and 'cannot be speculative.'" Id. (citation omitted). DiLuigi alleges injuries in the form of time spent on preventative measures, and he points to various fraudulent charges that he incurred. [CAC ¶¶ 88–89]. But "lost time" is not an "ascertainable loss", and DiLuigi concedes the fraudulent charges in question were reimbursed.[33] In re Rutter's, 511 F. Supp. 3d at 541 (explaining "lost time" and reimbursed costs not cognizable); see [CAC ¶ 88]. The Court need go no further; the failure to plead an ascertainable loss is ground for dismissal of a PUTPCPL claim. Maximus's motion is **GRANTED** as to Count 17.

xx. South Carolina Data Breach Security Act

In Count 26 against Delta Dental, Plaintiff Tillman alleges a violation of the South Carolina Data Breach Security Act. Delta Dental urges two grounds for dismissal.

First, Delta Dental argues that Tillman's stolen information does not qualify as "personal identifying information" under the statute. [Delta Dental Mem. at 84]. Referring to a direct quotation in the Bellwether Complaint from the data breach notice Delta Dental sent to Tillman,

[33] In his Opposition, DiLuigi supposes that the allegation that he had to "drive home from Georgia" to collect a replacement credit card sent to him in the mail should qualify as an ascertainable loss. [CAC ¶ 88]; see [Opp. to Maximus at 81]. But DiLuigi offers no context, legal authority, or explanation for his position, leaving only the bare allegation that a replacement credit card was mailed to him while he was away from his home, such that he could not retrieve it until he returned to his home. There is no obvious connection between these circumstances and any quantifiable loss that would be sufficient to state a claim for damages under the PUTPCPL.

Delta Dental argues that only Tillman's "date of birth and health insurance information" were stolen, [Delta Dental Mem. at 84 (quoting CAC ¶ 646)], which do not meet the statutory criteria.[34] Tillman contends she should be entitled to discovery because the nature of the information taken is "only known to Plaintiff Tillman through [Delta Dental's] notice letter, and the generality of 'health insurance information' makes it plausible that her PII . . . was breached." [Delta Dental Opp. at 66].

The Court agrees that Tillman should be given the opportunity to develop a fuller picture of the facts. Unlike some states, the South Carolina data breach law does not require any particular content in a notification letter, and as such, does not require a sender to disclose the particular types of information that have been affected by a breach. Compare S.C. Ann. § 39-1-90, with, e.g., N.Y. Gen. Bus. § 899-aa(7) (requiring notice to include "a description of the categories of information that were . . . accessed or acquired by a person without valid authorization"). Accordingly, it is plausible that the disclosure of "health insurance information" as described in Delta Dental's notice may have included information that could satisfy the statutory criteria.

Delta Dental also posits that Tillman has not alleged any injury stemming from delayed notification. [Delta Dental Mem. at 84]. Tillman alleges that Delta Dental learned about the data breach on June 1, 2023, but only notified her in a letter dated February 9, 2024. [CAC ¶ 646].

[34] South Carolina's data breach law defines "personal identifying information" as a person's "first name or first initial and last name" together with at least one of the following: "(a) social security number; (b) driver's license number or state identification card number . . . ; (c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or (d) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual." S.C. Code Ann. § 39-1-90(D)(3).

Setting aside whether the eight-month delay constituted a violation of the statute,[35] Tillman has plausibly alleged that if not for the "delay[] in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach." [CAC ¶ 655]. At this stage, her allegations that "delay prevented [her] from taking steps to protect [her] personal information from identify theft" adequately states an injury. Solara, 613 F. Supp. 3d at 1300; see also Dusterhoft v. OneTouchPoint Corp, No. 22-cv-00882, 2024 WL 4263762, at *20 (E.D. Wis. Sept. 23, 2024) (allowing South Carolina Data Breach Security Act claim to proceed based on three-month delay and allegation of injury resulting from the delay). Delta Dental's motion to dismiss Count 26 is **DENIED**.

xxi. Vermont Consumer Fraud Act

PBI contends that it cannot be held liable for Plaintiff Marshall's claim under the Vermont Consumer Fraud Act ("VCFA") because it lacks any relationship to her, as required under the statute. [PBI Mem. at 80].

Marshall alleges that she is a consumer because she "agree[d] to pay for products and services from users of MOVEit software," TIAA, who in turn paid PBI, in part "for data security protection they did not receive from Progress." [CAC ¶ 1773]. These allegations are insufficient to bring Marshall within the ambit of the statute as a consumer.

"A 'consumer' under the VC[F]A is someone who 'pay[s] consideration for goods or services' in some way." Mongeon v. KPH Healthcare Servs., Inc., No. 21-cv-00195, 2022 WL 1978674, at *3 (D. Vt. 2022) (alteration in original) (quoting Vt. Stat. Ann. § 2451a(1)). Here, Marshall fails to allege she is a "consumer" of services rendered by PBI. Although Vermont law

[35] A defendant violates the South Carolina Data Breach Security Act if it fails to disclose a breach in "the most expedient time possible and without unreasonable delay." S.C. Code Ann. § 39-1-90(A).

only requires "some relationship," not "strict privity," Bellwether Cmty. Credit Union v. Chipotle Mexican Grill, 353 F. Supp. 3d 1070, 1097 (D. Colo. 2018)), there must, nevertheless be a threshold showing that the plaintiff is a consumer within the meaning of the statute. Marshall nowhere alleges that she is a "purchaser" of the death-matching services PBI provides. Thus, it appears, PBI is not one of "the parties that [she] paid for services." Id. at 1098.

The court recognizes that the VCFA has been "liberally construed" to "include direct and indirect purchasers with no privity requirement." Mongeon, 2022 WL 1978674, at *3 (internal quotation marks omitted) (quoting Elkins v. Microsoft Corp., 817 A.2d 9, 13 (Vt. 2002)). Such a broad reading of the VCFA effectuates the statutory purpose of "allow[ing] the consumer to reach the person who committed the consumer fraud." Madowitz v. Woods at Killington Owners' Ass'n, 93 A.3d 571, 581 (Vt. 2014). Such "liberal construction," however, "does not allow [courts] to stretch the [statute's] language beyond legislative intent." Mongeon, 2022 WL 1978674, at *3 (first alteration in original) (quoting Elkins, 817 A.2d at 13). In no reasonable sense of the terms can Marshall be called a "consumer" of PBI's services.

In a parallel argument, TIAA contends that Marshall has failed to plead facts supporting causation under the VCFA. [PBI Mem. at 64]. "The section of the statute providing for a private right of action . . . requires a 'consumer' to show either (1) reliance on a deceptive act in contracting for goods or services or (2) damages or injury from an unfair or deceptive act." Dernier v. Mortg. Network, Inc., 87 A.3d 465, 481 (Vt. 2013). Marshall's claim against TIAA fails for lack of any plausible allegation of causation; she does not allege that she viewed or otherwise relied on any of the allegedly misleading statements, nor does she otherwise allege that she suffered an injury caused by any such misstatement. The motion to dismiss Count 22 against PBI and TIAA is **GRANTED**.

xxii. Virginia Consumer Protection Act and Virginia Data Breach Notification Law

Genworth contends that Count 23 should be dismissed because the Virginia Consumer Protection Act ("VCPA") exempts "insurance companies regulated and supervised by the State Corporation Commission." Va. Code Ann. § 59.1-199(4). The Virginia Data Breach Notification Act claim contains a materially identical limitation. Id. § 182-186.6(K). The Court takes judicial notice that this is applicable to Genworth,[36] and Genworth's motion to dismiss Counts 23 and 24 is **GRANTED**.

Maximus also contends that Count 18 must be dismissed against it because it is not a "supplier" in connection with a consumer transaction, as required by the VCPA. [Maximus Mem. at 63]. The VCPA prohibits certain "fraudulent acts or practices committed by a supplier in connection with a consumer transaction." Va. Code Ann. § 59.1-200(A). The statute defines "Supplier" as "a seller, lessor, licensor, or professional that advertises, solicits, or engages in consumer transactions, or a manufacturer, distributor, or licensor that advertises and sells, leases, or licenses goods or services to be resold, leased, or sublicensed by other persons in consumer transactions." Id. § 59.1-198. "Consumer transaction," in turn, is defined, in relevant part, as "[t]he advertisement, sale, lease, license, or offering for sale, lease, or license, of goods or services to be used primarily for personal, family, or household purposes." Id.

Maximus contends that "Plaintiffs offer no allegations showing that Maximus sold, leased, or licensed any goods or services to them or to consumers generally and therefore their VCPA claims must be dismissed." [Maximus Mem. at 65]. In response, Plaintiffs assert that

[36] See Commonwealth of Virginia State Corporation Commission Bureau of Insurance, Examination Report of Genworth Life and Annuity Insurance Company (Dec. 31, 2023), https://www.scc.virginia.gov/media/sccvirginiagov-home/regulated-industries/insurance/insurance-companies/for-companies/-company-financial-reporting/65536.pdf.

"[t]he VCPA includes upstream suppliers of services within the definition of 'supplier.'" [Maximus Opp. at 68]. Whether the consumer relationship needs to be "direct," however, is beside the point. Maximus's position is that it is not a "supplier" at all. A review of the CAC supports Maximus's position. According to the Complaint, Maximus is a government contractor that supports government benefit programs by providing "medical evaluations, review of eligibility appeals, enrollment assistance, data analysis, and IT and consulting services." [CAC ¶ 2932]. The Complaint particularly emphasizes Maximus's role in administering Medicare eligibility appeals. [Id. ("Regarding Medicare specifically, Maximus reviews 'more than 600,000 appeals claims a year for Medicare' patients who experienced 'health insurance denials.'")]; [id. ¶ 2933 ("Maximus is the largest provider of government-sponsored benefit appeals programs in the United States.")]. In the absence of specific allegations or arguments to the contrary, the Court cannot find that the government programs that Maximus helps administer involve "consumer transactions." Moreover, the particular appeals and other benefit-management services that Maximus is alleged to provide are plainly not "resold, leased, or sublicensed by other persons in" in the course of any such "consumer transaction[]." Va. Code Ann. § 59.1-198. Maximus's motion to dismiss Count 18 is **GRANTED**.

Maximus also asks the Court to dismiss Count 19, alleging liability under the Virginia Data Breach Notification Law, on the ground that no plaintiff is a resident of Virginia. Plaintiffs concede that none of them are Virginia residents, but say that the "statute does not explicitly preclude non-residents from bringing claims" and "only requires that a '[b]reach of the security system' cause[d] 'identity theft or other fraud to any resident of the Commonwealth.'" E.g., [Opp. to Maximus at 65 (quoting Va. Code Ann. § 18.2-186.6)].

The text of the VDBL directly refutes Plaintiffs' argument. The VDBL provides that "an individual" may "recover[] direct economic damages" arising "from a violation" of the statute.[37] Va. Code. Ann. § 18.2-186.6(I). After a qualifying data security incident, the statute requires the breached entity to "disclose [the] breach . . . to the Office of the [Virginia] Attorney General and any affected resident of the Commonwealth without unreasonable delay." Id. § 18.2-186.6(B) (emphasis added). Inasmuch as the statute only requires notification to Virginia residents, it follows that only Virginia residents can suffer violations of the statute. The statutory text supports Maximus, and the Court agrees with what other MDL courts have found obvious: the VDBL "authorizes a Virginia resident to recover direct economic damages," but does not apply to non-residents. Cap. One, 488 F. Supp. 3d at 416. The lack of a Virginia plaintiff here is fatal to Plaintiffs' claim. Maximus's motion to dismiss Count 19 is **GRANTED**.

i. Washington Data Breach Notice Act

Plaintiff Soto brings a Washington Debt Data Breach Notice Act ("WDBNA") claim against Milliman. [CAC ¶¶ 2382–90]. Milliman argues that the WDBNA only applies to residents of the state. [PBI Mem. at 60]; see Wash. Rev. Code § 19.255.010(1); Guy v. Convergent Outsourcing, Inc., No. 22-cv-1558, 2023 WL 4637318, at *9 (W.D. Wash., July 20, 2023) (granting motion to dismiss a WDBNA claim because "[e]ven if such a claim had been asserted, the Court would dismiss it because none of named Plaintiffs is a resident of

[37] It is unclear whether this language purports to provide an independent private right of action, or merely allows a plaintiff to rely on a violation of the VDBL to establish liability under another statute, such as the Virginia Consumer Protection Act. Section I states that "the Attorney General may bring an action to address violations of this section" including by "impos[ing] a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation." Va. Code Ann. § 18.2-186.6(I). The statute further provides, however, that "[n]othing in this section shall limit an individual from recovering direct economic damages from a violation" of the statute. Id. The Court need not decide whether the latter language creates a cause of action because only a Virginia resident can suffer a violation of the statute.

Washington—a requisite element"). Plaintiff offers no response, see [PBI Opp. at 78 (mistakenly stating that "Milliman challenges Plaintiff Soto's claim 26 under the Washington Data Breach Notice Act . . . on only one basis: that it is insufficiently pled because it 'paraphras[es] or quot[es] statutory provisions' and is 'boilerplate,' in conclusory fashion . . . ." (emphasis added))]. PBI's motion to dismiss Count 26 is therefore **GRANTED**.

Plaintiff McClendon also brings a claim against Welltok and Virginia Mason for violation of the "WDBNA." [CAC ¶ 3793–806]. The statute requires disclosure of a data breach within "the most expedient time possible . . . no more than thirty calendar days after the breach was discovered." Wash. Rev. Code Ann. § 19.255.010(8). Defendant Virginia Mason, a medical center, claims that this provision does not apply because Defendant Progress, not the VCE, "discovered" the breach, thus placing Defendant Virginia Mason's acts outside the scope of the statute. [Welltok Mem. at 85]. While the Amended Consolidated Complaint states that "Progress discovered the Data Breach," [CAC ¶ 369], Virginia Mason was notified of the breach in September 2023, [CAC ¶ 3469]. This date can reasonably be considered when Virginia Mason "discovered the breach."

Defendants dispute that Plaintiff pleads any facts to demonstrate that its notification of the breach to Plaintiff was untimely. [Welltok Reply at 38]. Welltok was informed of the Data Breach on July 26, 2023, and Plaintiff received a Notice Letter informing her of the Data Breach on December 1, 2023. [CAC ¶¶ 367, 3482]. "[I]t took Welltok and Virginia Mason over four months to notify Plaintiff McClendon of the Data Breach's occurrence." [CAC ¶ 370]. The fact that notification to Plaintiff took over four months is clearly outside the thirty-day window provided for in the WDBNA. Wash. Rev. Code Ann. § 19.255.010(8).

Defendants, however, also claim that Plaintiff fails to demonstrate that this delay in notification caused distinct injury beyond that which she suffered due to the Data Breach itself, and that such an incremental injury is a requirement under the WDBNA. [Welltok Mem. at 86]. The parties dispute the case law on such a requirement. Defendants cite several cases in support of their position. See [Welltok Mem. at 85 (citing Grigsby v. Valve Corp., No. C12-0553JLR, 2013 WL 12310666, at *5 (W.D. Wash. Mar. 18, 2013) (holding that, under the WDBNA, a plaintiff must show that he was "injured due to the interval between the hacking incident and [the Defendant's] notice of the incident and not just that he was injured by the hacking incident alone")]; [Welltok Reply at 38–39 (citing In re Flagstar Dec. 2021 Data Sec. Incident Litig., No. 22-cv-11385, 2024 WL 5659583, at *14 (E.D. Mich. Sept. 30, 2024) (dismissing WDBNA claim because "plaintiffs c[ould not] allege injury resulting from the delayed notification") (emphasis in original); Sony Gaming II, 996 F. Supp. 2d 1010) (requiring a showing of incremental harm in a case concerning the California Database Breach Act, which "mirrors" the WDBNA)]. Plaintiff claims that the existence of this requirement is "murky," but cites no additional authority supporting that contention. [Welltok Opp. at 71]. The Court, therefore, agrees with Defendant that the weight of the authority suggests that Plaintiff must allege some distinct injury caused by the delay.

To that end, Plaintiff offers conclusory allegations that the delay in notification "deprived [her] of prompt notice of the Data Breach and [she was] thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze," [CAC ¶ 3803], and that, as a result, she "suffered incrementally increased damages separate and

distinct from those caused by the Data Breach itself," [CAC ¶ 3804]. See also [CAC ¶ 3474].[38] She fails, however, to "allege concrete fraud or identity [sic] that could have been prevented had the notification of the breach come sooner." In re Flagstar, 2024 WL 5659583, at *14. Absent pleading that the Plaintiff suffered harm separate and unique from the damages wrought by the Data Breach itself, Plaintiff has failed to sufficiently allege a claim under the WDBNA and Welltok and Virginia Mason's motion to dismiss Count 21 is therefore **GRANTED**.

ii. Washington Consumer Protection Act

Plaintiff Soto also brings a claim against Milliman under the Washington Consumer Protection Act ("WCPA"). [CAC ¶¶ 2373–81]. "To prevail on a CPA claim, a plaintiff must prove: (1) an unfair or deceptive act or practice, (2) in trade or commerce, (3) that impacts the public interest, (4) which causes injury to the party in his business or property, and (5) which injury is causally linked to the unfair or deceptive act." Zander v. New Hampshire Indem. Co., No. 05-cv-05154, 2006 WL 2243035, at *3 (W.D. Wash. July 26, 2006). Milliman argues that Plaintiff Soto has failed to allege causation, which they argue is a required element under the WCPA. [PBI Mem. at 64]. The Court's own examination of Soto's allegations reveals that his only allegations of proximately caused losses are lost time and emotional distress. [CAC ¶¶ 824, 826], which are plainly not injuries to business or property. He does not allege that he has suffered identity theft, spent money on credit monitoring or other remedial measures, or suffered

[38] In subsequent briefing, Plaintiff claims that "Defendants' delay allowed Plaintiff McClendon's Private Information to be exposed for months before Plaintiff had any idea that her information was compromised, preventing her from taking action to stop or mitigate any misuse of her Private Information (such as enrolling in her current credit monitoring with IDNotify earlier)." [Welltok Opp. at 71] (emphasis in original). This pleading's characterization of the allegations confirms that the allegations are not sufficiently concrete to establish an injury distinct from the injuries associated with the Data Breach.

any other out-of-pocket loss. Nor does he allege facts supporting any inference of causation. PBI's motion to dismiss Count 25 is therefore **GRANTED**.

Plaintiff McClendon likewise pleads that Welltok and Virginia Mason violated the WCPA. [CAC ¶¶ 3807–16]. McClendon alleges these Defendants failed to protect against and properly notify Plaintiff of the Data Breach, [CAC ¶ 3811], resulting in injuries to her personal information and privacy as well as associated financial expenses. [CAC ¶ 3815]. Defendants object to Plaintiff's WCPA claim, asserting that it fails to plausibly allege three elements of the statute: (1) "an unfair or deceptive" practice, (2) "which causes injury to . . . business or property," and (3) causation. Zander, 2006 WL 2243035, at *3. Defendants also claim that "WCPA defendants are typically businesses whose systems were actually impacted," [Welltok Mem. at 87], but does not give the Court any reason to believe that Virginia Mason is an unfit—rather than simply an atypical—Defendant. Particularly given that the WCPA is to be read broadly to cover a wide array of practices, absent evidence otherwise, it is reasonable to include Virginia Mason in this claim. Veridian Credit Union v. Eddie Bauer, LLC, 295 F. Supp. 3d 1140, 1161–62 (W.D. Wash. 2017) ("The Washington Legislature directs that the CPA 'shall be liberally construed [so] that its beneficial purposes may be served.'") (quoting RCW 19.86.920).

Defendants claim that Plaintiff fails to plead the existence of unfair or deceptive practices, a requirement of the WCPA. [Welltok Mem. at 87–88]. Failure to reasonably protect personal information can constitute an unfair practice under the WCPA. Guy, 2023 WL 4637318, at *8 ("[T]he failure to take proper measures to secure [personal identifying information] can constitute an unfair act under the CPA."); Veridian, 295 F. Supp. 3d at 1161 (holding that "fail[ure] to provide reasonable cyber security measures to protect the account

information on . . . customers' credit and debit cards constitutes either an 'unfair or deceptive act or practice' under the CPA.").

Plaintiff claims that Defendants' failures to "implement and maintain reasonable security and privacy measures," "identify foreseeable security and privacy risks, and remediate identified security and privacy risks," and "comply with common law and statutory duties" were each "a direct and proximate cause of the Data Breach." [CAC ¶ 3811]. More specifically, Plaintiffs allege that Welltok did not "take proper measures to protect" personal information, Veridian, 295 F. Supp. 3d at 1161, by "failing to employ adequate vendor screening and vetting, including of Progress and its MOVEit Transfer application," [CAC ¶ 3385]. Furthermore, Welltok and Virginia Mason allegedly "should have but did not vet Progress or its MOVEit Transfer application," [CAC ¶ 3387], and "failed to ensure Progress employed and maintained adequate cybersecurity measures," [CAC ¶ 3388]. Welltok also allegedly failed to take recommended precautions for securing data passing through MOVEit software. [CAC ¶¶ 3453–61]. The Data Breach led to the unauthorized sharing of Plaintiff McClendon's "name, address, date of birth, some clinical information, patient ID, and health insurance information." [CAC ¶ 367]. These allegations are sufficient to make out the first element of a WCPA claim. Defendants' only argument to the contrary is that Plaintiff has not pled a deceptive practice; they make no attempt to refute that Plaintiff has alleged an unreasonable practice as described above. [Welltok Mem. at 87]. Given that the WCPA only requires a Plaintiff to demonstrate unfair or deceptive practices, at this stage the Court need not reach the question of whether Plaintiff sufficiently alleged that Defendants engaged in deceptive practices under the Rule 9(b) pleading standard.

Defendants further argue that Plaintiff fails to "satisfy the injury requirement for a claim for unfair or deceptive conduct under the WCPA," [Welltok Mem. at 87], and claim that the

alleged injuries were not "a result of [defendant's] conduct." [Id. at 88 (quoting Saeedy v. Microsoft Corp., No. 23-cv-1104, 2023 WL 8828852, at *6 (W.D. Wash. Dec. 21, 2023)]. More specifically, they assert that Plaintiff McClendon fails to satisfy the injury prong of the WCPA because she only proffers "bareboned allegations [which] do not plausibly show that BP McClendon has lost money or property under the above authorities." [Id.].

In order the satisfy the fourth prong of the WCPA, "[t]he injury involved need not be great, but it must be established." Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co., 719 P.2d 531, 539 (Wash. 1986). Plaintiff must demonstrate an "injury to a person's business or property."[39] Panag v. Farmers Ins. Co. of Washington, 204 P.3d 885, 889 (Wash. 2009) (en banc) (emphasis added). Under Washington law, "[p]ersonal injuries, as opposed to injuries to 'business or property,' are not compensable and do not satisfy the injury requirement." Panag, 204 P.3d at 899.

Plaintiff McClendon claims she has suffered, and is at heightened risk of suffering, losses in the form of

> the unauthorized use of her stolen Private Information . . . ; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private Information; and injury to her privacy.

[CAC ¶ 384]. She also alleges that, due to the Data Breach, she "has experienced other forms of spam and phishing emails, texts, and phone calls on a daily basis." [CAC ¶ 377]. Plaintiff now

[39] The Court recognizes some discrepancy in how courts have chosen to interpret "business or property." Compare Saeedy, 2023 WL 8828852 at *6 (precluding WCPA claim against Microsoft for failure to establish personal loss of money or property); with Guy, 2023 WL 4637318, at *8 (finding that lost value of personal identifying information may constitute an injury). Given the liberal construction of the WCPA, the Court finds it appropriate to let the claim move forward at this stage.

"pays $100 annually in out-of-pocket costs for credit monitoring services with IDNotify." [CAC ¶ 378]. Although Plaintiff's loss of privacy and time injuries are arguably personal and therefore not compensable under the WCPA, Gragg v. Orange Cab Co., 942 F. Supp. 2d 1111, 1119 (W.D. Wash. 2013) ("[A]n invasion of privacy is a 'personal' injury, rather than a 'business or property' injury."), her claims of expenses incurred scrutinizing her financial information and lost value of personal data are sufficient to satisfy the injury requirement of the WCPA. See [CAC ¶ 378–85]; Guy, 2023 WL 4637318, at *8 (finding that loss of value of personal identifying information is "sufficient to show an injury," however, lost time—while evidence of damages—may not be evidence of injury). The costs Plaintiff has incurred paying for a credit monitoring service may also constitute an injury under the WCPA.[40] Therefore, at this stage, Plaintiff's allegations adequately demonstrate injury.

Finally, Plaintiff must demonstrate "[a] causal link . . . between the unfair or deceptive acts and the injury suffered by plaintiff." Hangman, 719 P.2d at 539; see also In re Flagstar, 2024 WL 5659583, at *15 ("[E]ach Plaintiff must be able to allege facts connecting their alleged injuries to the unlawful, unfair, deceptive, or fraudulent actions of Flagstar."); Robertson v. GMAC Mortg. LLC, 982 F. Supp. 2d 1202, 1209 (W.D. Wash. 2013), aff'd on other grounds,

[40] Defendants cite this Court's decision in Scifo v. Alvaria, Inc. finding that, "[w]here, as here, Plaintiffs have not shown an imminent risk of identity theft, prophylactic costs to mitigate such a risk do not constitute an independent injury sufficient to support standing." No. 23-CV-10999, 2024 WL 4252694, at *5 (D. Mass. Sept. 20, 2024). However, where "Plaintiffs plead that due to the substantial risk their data will be misused, they will need to continue monitoring their accounts in the future," it is plausible that, "[c]osts of future credit monitoring are also cognizable injuries." LastPass, 742 F. Supp. 3d at 123. In present case, Plaintiff "has experienced other forms of spam and phishing emails, texts, and phone calls on a daily basis," [CAC ¶ 377], which may give rise to reason to believe she is at risk of "an imminent risk of identity theft," Scifo, 2024 WL 4252694, at *5, and thus Plaintiff's costs associated with credit monitoring may be considered a cognizable injury. Given the other identified injuries to "business or property" identified above, the Court need not settle this question at this stage.

702 F. App'x 595 (9th Cir. 2017) (establishing a "but for" standard between the unfair or deceptive practice and the injury suffered); Indoor Billboard/Washington, Inc. v. Integra Telecom of Washington, Inc., 170 P.3d 10, 22 (Wash. 2007) ("A plaintiff must establish that, but for the defendant's unfair or deceptive practice, the plaintiff would not have suffered an injury."); Woodell v. Expedia Inc., No. C19-0051JLR, 2019 WL 3287896, at *11 (W.D. Wash. July 22, 2019) ("Proximate cause is a required element of a CPA claim."). Defendants claim that Plaintiff was never exposed to the alleged unfair or deceptive practices and thus the unfair conduct was not a proximate cause of her injury [Welltok Reply at 40 ("McClendon does not allege that she saw, let alone relied on, any representation by Virginia Mason or Welltok, a necessary element of her WCPA claim.")].

The Court accepts, for present purposes, Plaintiff's claim that Defendants' failure to take proper measures to protect her personal information amounts to an unfair practice within the scope of the WCPA, and that any lost value of personal information constitutes an injury. Plaintiff McClendon asserts that the injuries sustained occurred "[a]s a direct and proximate result of the Data Breach." [CAC ¶ 379]; See also [id. 384–85]. Given the extensive measures that she has taken to secure and protect her personal information, [CAC ¶ 380], it is a reasonable inference that, but for Defendants failure to take reasonable measures to protect Plaintiff's personal information, she would not have experienced the invasions caused by the Data Breach. Thus, Plaintiff would not have lost the value of her personal data and would not have incurred "expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity." [CAC ¶ 384]. Taking these statements as true and in the light most favorable to the Plaintiff, the Court finds that Defendants' unfair or deceptive practices were a

proximate cause of injuries to "business or property" suffered by Plaintiff McClendon. Welltok's motion to dismiss Count 22 is **DENIED**.

iii. Wisconsin Deceptive Trade Practices Act

MLIC urges dismissal of the Wisconsin Deceptive Trade Practices Act ("WDTPA") claims alleged against it on the ground that Plaintiff Soto is a resident of Florida, not Wisconsin, and thus, no plaintiff is a resident of Wisconsin. Pursuant to the WDTPA,

> No person, firm, corporation or association, or agent or employee thereof . . . shall make, publish, disseminate, circulate, or place before the public, or cause, directly or indirectly, to be made, published, disseminated, circulated, or placed before the public, in this state . . . an advertisement, announcement, statement or representation of any kind to the public . . . which advertisement, announcement, statement or representation contains any assertion, representation or statement of fact which is untrue, deceptive or misleading.

Wisc. Stat. § 100.18(1). Although no Wisconsin Supreme Court case appears to have yet confronted the issue raised by MLIC, the Wisconsin Court of Appeals has addressed whether the statute reaches conduct by in-state defendants that only affects out-of-state consumers with respect to lawsuits initiated by state attorneys general under the WDTPA. See State v. Talyansky, 995 N.W.2d 277, 283 (Wisc. Ct. App. 2023). The court held that the plain language of "[t]he statute does not pr[e]scribe where the recipient or consumer must reside," and concluded that "the State can enforce [it] against Wisconsin businesses," like MLIC, "that reach consumers outside of the state." Id. The court noted it's disapproval of the contrary interpretation of § 100.18(1) raised in the only case MLIC cites in support of its position. See id. at 284 n.6 (describing as "unpersuasive" Hydraulics International, Inc. v. Amalga Composites, Inc., No. 20-cv-00371, 2022 WL 4273475, at *6 (E.D. Wisc. Sept. 15, 2022)).

Neither the intermediate appellate decision (Talyanksy) nor the district court decision (Hydraulics) is binding here. See Andrew Robinson Int'l, Inc. v. Hartford Fire Ins. Co., 547 F.3d 48, 55 (1st Cir. 2008) ("While decisions of a state's intermediate appellate court are not binding on a federal court sitting in diversity, such opinions are entitled to some weight."). That said, the reasoning of Talyansky is more persuasive in its reading of the statutory language. While a legislature could, of course, delimit the reach of its statutes on the basis of victim residence, mere silence on the point seems a poor way to achieve that result. The contrast with the Virginia statute discussed supra, which does expressly refer to residents of that Commonwealth, is instructive.

MLIC also contends that Soto has not plausibly alleged "a causal connection between the untrue, deceptive, or misleading statement and the pecuniary loss" that Soto suffered. K&S Tool & Die Corp. v. Perfection Mach. Sales, Inc., 732 N.W.2d 792, 802 (Wisc. 2007); [PBI Bellwether Mem. at 45]. Soto quibbles that K&S Tool involved an appeal from a jury verdict in a case that did not involve a data breach, but the point is that Soto fails to identify any allegation in the CAC to support either causation or pecuniary loss. [Opp. to PBI at 79]. His only allegations of loss are lost time and emotional distress. [CAC ¶¶ 824, 826]. He does not allege that he has suffered identity theft, spent money on credit monitoring or other remedial measures, or suffered any other out-of-pocket loss.[41] Nor does he allege facts supporting any inference of causation.

The motion to dismiss the WDPTA claim is **GRANTED**.

[41] At most he alleges that he "anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach," [CAC ¶ 827], but a hypothetical future cost is not a recoverable pecuniary loss.

iv. Declaratory Judgment Act

The non-Progress Defendants argue for dismissal of Plaintiffs' request for declaratory relief primarily on the ground that it is duplicative of their negligence and contract claims. See, e.g., [PBI Mem. at 83]. Plaintiff's tort and contract claims, however, seek only retrospective relief. Their request for declaratory judgment, by contrast, is premised on allegations that the "security measures on [the] MOVEit software remain inadequate," [CAC ¶ 1813], and that as a result, "the risk remains that further compromises of [Plaintiffs'] Private Information will occur in the future," [CAC ¶ 1814]. An allegation of "continued inadequacy of [a] Defendant['s] security measures" suffices to support a claim for declaratory judgment in a data breach case. Unite Here, 740 F. Supp. 3d at 388 (quoting Cap. One, 488 F. Supp. 3d at 414–15).[42] Accordingly, the PBI Bellwether Defendants' motion to dismiss Count 28, Delta Dental's motion to dismiss Count 12, Maximus's motion to dismiss count 4, and the Welltok Bellwether Defendants' motion to dismiss Count 6 are **DENIED**.

IV. CONCLUSION

For the reasons stated above:

- The PBI Bellwether Defendants' motion is **GRANTED** on Counts 3–4, 7, 9, 11, 12, 14, 15–17, 19–27; **GRANTED IN PART** on Count 2, **DENIED** on Counts 1, 5–6, 8, 10, 13, 18, and 28.

[42] As discussed supra, to the extent the non-Progress Defendants invoke this Court's standing ruling regarding injunctive relief as a ground for rejecting their declaratory judgment claim, [Mem. at 64]; see also [ECF No. 1304 at 6 n.3], that argument is rejected.

- The Delta Dental Bellwether Defendants' motion is **GRANTED** on Counts 2, 3–9, 11, 13–14, 16–17, 20, and 24–25; **GRANTED IN PART** on Counts 17–18, and **DENIED** on Counts 1, 10, 12, 15, 17, 19, 23, and 26.
- The Maximus Bellwether Defendants' motion is **GRANTED** on Counts 5–9, 12, 14–15, and 17–19; **GRANTED IN PART** on Count 3, and **DENIED** on Counts 1–2, 4, 10–11, 13, and 16.
- The Welltok Bellwether Defendants' motion is **GRANTED** on Counts 4–5, 9, 11–15, 17, and 21; **GRANTED IN PART** on Count 2, and **DENIED** on Counts 1, 3, 6–8, 10, 16, 18–20, and 22.

SO ORDERED.

July 31, 2025

/s/ Allison D. Burroughs
ALLISON D. BURROUGHS
U.S. DISTRICT JUDGE