UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Arthur J. Gallagher Data Breach Ligation	Case No. 22-cv-137
	Judge Mary M. Rowland

MEMORANDUM OPINION AND ORDER

In 2020, insurance brokers Defendants Arthur J. Gallagher (AJG) and Gallagher Basset Services (GBS) experienced a cybersecurity attack to their internal systems. After receiving notices of the data breach from Defendants, Plaintiffs—former clients and employees—claim injuries under common law, consumer protection statutes, and data notification statutes. Plaintiffs bring putative class actions seeking to represent a nationwide class and state subclasses. Defendants move to dismiss the two complaints in this consolidated case. [2] [4]. For the reasons explained below, this Court grants in part and denies in part Defendants' motions.

I. Background

This Court accepts as true the following facts from the consolidated amended complaint (CC) and the May complaint (MC).[1] *See Wagner v. Teva Pharm. USA, Inc.*, 840 F.3d 355, 358 (7th Cir. 2016). Because Plaintiffs' complaints contain similar

[1] For efficient case management purposes, the Court consolidated several pending related cases under this master case number. The majority of the Plaintiffs have presented their case in a consolidated amended complaint (CC), found at ECF No. 25 in case 21-cv-4056. The other Plaintiff, Leslie May's complaint (MC), is located at ECF No. 1-1 in case 21-cv-5851.

allegations and concern similar claims, this Court will sometimes cite to one complaint for a proposition that applies to all Plaintiffs. Unless otherwise indicated, citations to docket numbers refer to filings in the master case, case number 21-cv-4506.

A. General Allegations

Plaintiffs John Parsons, Adrian Villalobos, Christopher Caswell, Robert Davie, Peter Horning, Julia Kroll, Amanda Marr, Brent McDonald, Jonathan Mitchell, Jason Myers, John Owens, Alan Wellikoff, Chandra Wilson, Arda Yeremian, Tracey Block, and Leslie May claim that Defendants injured them by failing to secure and safeguard their personally identifiable information and/or protected health information. *See generally* CC; MC. Defendant AJG is a leading insurance brokerage, risk management, and HR & benefits company. CC ¶ 2. AJG's global group of companies and partners includes Defendant GBS, a third-party administrator and claims manager. *Id.* ¶ 3.

Plaintiffs allege that, from June 3 to September 26, 2020, an unknown party accessed certain segments of AJG's network, including segments at GBS, during a ransomware event (the Data Breach). *Id.* ¶ 5. During the Data Breach, the attacker accessed records containing the personal information of more than three million individuals. *Id.* ¶ 6. On or around September 26, 2020, Defendants detected the ransomware event. *Id.* ¶ 7. Around June 30, 2021, Defendants began notifying some class members and various states' Attorneys General of the Data Breach. *Id.* ¶¶ 8, 9.

Plaintiffs claim the Data Breach resulted from Defendants' failure to properly

secure and safeguard their personally identifiable information (PII), including names, social security numbers, tax ID numbers, driver's licenses, passport or other government identification numbers, dates of birth, usernames and passwords, employee ID numbers, financial or credit card information, and/or electronic signatures. *Id.* ¶ 1. Plaintiffs also claim that Defendants failed to safeguard their protected health information (PHI), such as medical records or account numbers and biometric information. *Id.* Plaintiffs allege that the Data Breach has resulted in the unencrypted PII and PHI of Plaintiffs and class members ending up for sale on the "dark web as that is the *modus operandi* of hackers." *Id.* ¶ 59. Plaintiffs assert that Defendants should have implemented better measures that prevent and detect ransomware attacks. *Id.* ¶ 62.

B. Named Plaintiffs' Experiences

Plaintiff Parsons worked for AJG in Louisiana from January 1996 through April 1999. *Id.* ¶ 96. Parsons trusted his PII and PHI to AJG, who retained Plaintiff's name and social security number in its system during the time of the Data Breach. *Id.* ¶ 97. Parsons received notice of the Data Breach on July 18, 2021; the notice stated that Parsons' name and social security number were among the information accessed or acquired during the Data Breach. *Id.* ¶ 99. As a result, Parsons spent time verifying the legitimacy of the Data Breach notice and self-monitoring his accounts. *Id.* ¶ 100. Parsons experienced a "substantial increase" in suspicious calls, emails, and text messages which he believes is related to the Data Breach. *Id.* ¶ 106.

Plaintiff Villalobos worked for Prolacta Bioscience in California from

September 2015 to August 2019. *Id.* ¶ 108. In connection with his employment, Villalobos entrusted his PHI and/or PII to Defendants, "possibly through a third-party that provided human resources services to Prolacta." *Id.* ¶ 109. Villalobos received Defendants' notice of the Data Breach in August 2021; the notice stated that his name, medical diagnosis, medical treatment information, and medical claim information were accessed or acquired during the Data Breach. *Id.* ¶ 111.

Plaintiff Caswell worked for Saddle Creek Logistics Services from 2016 to December 2020. *Id.* ¶ 119. In connection with that employment and a workers compensation claim, Caswell entrusted his PII and/or PHI to Defendants. *Id.* ¶ 120. Caswell's notice of the Data Breach stated that his "personal information" was among the information accessed or acquired during the Data Breach. *Id.* ¶ 122.

Plaintiff Davie worked for Whirlpool Corporation in California from August 1998 to October 2008 and entrusted his PII and/or PHI to GBS as the third-party administrator for Whirlpool's workers compensation claims. *Id.* ¶¶ 130–31. The notice Davie received stated that his name, social security number, medical record number, medical diagnosis, medical treatment information, health insurance information, and medical claim information were accessed or acquired during the Data Breach. *Id.* ¶ 133. Davie also received a letter from Whirlpool stating that some of his employee information had been impacted during a ransomware attack affecting GBS. *Id.* Davie claims that, as a result of the Data Breach, he experienced an increase in suspicious phone calls and emails and purchased "Robokiller" for $4.99 per month from approximately July through September 2021 to address this problem. *Id.* ¶ 134.

Davie also experienced a decline in his credit score that he believes is, at least in part, due to a "hard inquiry" by ADT on his credit report; because Davie has not used ADT's services, he believes this unauthorized inquiry is related to the Data Breach. *Id.* ¶ 135.

From 2001 to 2003 and 2014 to 2019, Plaintiff Horning worked for the Pinellas County Sheriff's Office in Florida; from 2003 to 2014, Plaintiff worked for the Gulf Port Police Department, also in Florida. *Id.* ¶ 143. In connection with his employments, Horning entrusted his PII and PHI to Defendants, "possibly through Defendant's provision of workers' compensation insurance to either the Pinellas County Sheriff's Office or the Gulf Port Police Department or both." *Id.* ¶ 144. Horning received notice of the Data Breach around September 14, 2021, which stated that his name, medical diagnosis, and medical claim information was accessed or acquired. *Id.* ¶ 146. Horning has experienced a "substantial increase" in suspicious calls, emails, and text messages and believes these events are related to the Data Breach. *Id.* ¶ 153.

Plaintiff Kroll worked for the Glenbard School District in Illinois from August to November 2018 and entrusted her PII and/or PHI to Defendants, likely through the Suburban School Cooperative Insurance Pool. *Id.* ¶¶ 155–56. The notice Kroll received about the Data Breach stated that her name and medical claim information was accessed or acquired. *Id.* ¶ 158. Since the Data Breach, Kroll has experienced fraudulent charges on her credit card and an increase in suspicious calls and emails. *Id.* ¶ 159. The fraudulent charge made Kroll unable to purchase furniture. *Id.* Even

now, Kroll experiences difficulties when she uses her credit card to make larger purchases. *Id.*

Plaintiff Marr worked for Omni Hotels and Resorts in California from 2013 to 2019, and in connection with that employment, entrusted her PII and/or PHI to Defendants. *Id.* ¶ 168. Marr received notice of the Data Breach around July 21, 2021, and the notice informed her that her name, social security number, medical diagnosis, medical treatment information, medication information, health insurance information, and medical claim information were accessed or acquired during the Data Breach. *Id.* ¶ 170. Marr believes that, as a result of the Data Breach, a criminal used her identity to apply for unemployment benefits sometime during the summer of 2020. *Id.* ¶ 172. In addition, Marr has experienced an increase in scam emails and phone calls and a notice from "gotpwned.com" indicating that she needed to change her email passwords. *Id.* ¶ 173.

Plaintiff McDonald worked for Labor Finders in California from September 2018 through January 2019 and entrusted his PII and PHI to Defendants, possibly through Defendants' provision of workers' compensation insurance to Labor Finders. *Id.* ¶¶ 180–81. A July 21, 2021 notice informed McDonald that the Data Breach compromised his name, social security number, medical diagnosis, medical treatment information, and medical claim information. *Id.* ¶ 183. Since the Data Breach, McDonald experienced fraud and identify theft, which has led him being charged late fees by his bank, utility companies, and his landlord, *id.* ¶¶ 191–92.

Plaintiff Mitchell worked for Circle Home, Inc. in Massachusetts from May

2012 to present. *Id.* ¶ 198. Mitchell entrusted his PII and PHI to Defendants, possibly through their provision of workers' compensation insurance to Plaintiff's employer. *Id.* ¶ 200. He also received notice that his name and social security number were compromised during the Data Breach, and claims to have experienced a "substantial increase" in spam calls, emails, and texts which he believes is related to the Data Breach. *Id.* ¶¶ 202, 209.

Plaintiff Owens worked for the Montgomery County Fire and Rescue in Maryland from 1986–2014. *Id.* ¶ 211. Owens submitted multiple workers compensation claims from 2001 through 2011, and as part of that insurance process, entrusted his PII and/or PHI to Defendants. *Id.* ¶ 212. The Data Breach notice to Owens stated that his name and medical information were accessed or acquired. *Id.* ¶ 214. As a result of experiencing an increase in spam phone calls and emails after the Data Breach, Owens purchased and installed a spam phone system that cost $100.00. *Id.* ¶ 220.

Plaintiff Welikoff, a Maryland citizen, is "unaware of how Defendants came into possession of his PII." *Id.* ¶¶ 38, 223. Welikoff received a notice of the Data Breach in August 2021, stating that his name and medical information were among the information accessed or acquired. *Id.* ¶ 224. Since then, Welikoff has received text messages and password reset notifications from several of his accounts, indicating that unknown third parties have been attempting to access his accounts; an authorized third party also tried to access his bank accounts. *Id.* ¶ 225. Welikoff also received a notification from McAfee that his Comcast email address "was found on

the dark web." *Id.* ¶ 226.

Plaintiff Wilson worked for United Airlines in Colorado from 1997 to 2006, and again from June 2012 to present. *Id.* ¶ 235. Wilson entrusted her PII and/or PHI to Defendants, possibly in connection with one or more workers' compensation claims. *Id.* ¶ 236. The notice to Wilson stated that her name, social security number, medical diagnosis, medical treatment information, health insurance information, and medical claim information were among the information accessed or acquired during the Data Breach. *Id.* ¶ 238. Since the Data Breach, Wilson has suffered from identity theft. *Id.* ¶ 239. In February and March 2021, she discovered that someone had opened five utility accounts in her name using her social security number and date of birth in Texas at three different utility companies, Reliance Energy, TXU Energy, and First Choice Power. *Id.* Wilson alleges that, as a result, she has suffered adverse effects to her credit score, has been denied credit, and has spent money on LifeLock to protect her identity. *Id.* ¶ 241.

Plaintiff Yeremian worked for AJG in California from 2014 to 2017 and then again in 2020 for a couple of months. *Id.* ¶ 248. Yeremian received notice around August 10, 2021 that her name, social security number, and employee identification number were among the information accessed or acquired during the Data Breach. *Id.* ¶ 251. Yeremain claims that, as result of the Data Breach, she has experienced increased spam calls, a decrease in her credit score, and other actual damages. *Id.* ¶¶ 254–55, 259.

While employed as a flight attendant for Miami Air International in January

2017, Plaintiff Bock was injured while on the premise of a local hotel on a layover in North Dakota. *Id.* ¶ 263. In connection with her employment, Bock entrusted her PII and/or PHI to GBS as the third-party administrator to process her workers' compensation claims. *Id.* ¶ 264. The notice letter to Bock informed her that her name, medical diagnosis, and medical claim information were compromised during the Data Breach. *Id.* ¶ 266. Among other inconveniences, Bock had to replace her debit card twice as a result of the Data Breach. *Id.* ¶ 267.

Plaintiff May, a California resident, claims that in July 2021, she learned that her PII and PHI were accessed, viewed, and/or acquired by unauthorized individuals through the Data Breach. MC ¶ 9. May provided her PII to Defendants in the course of purchasing "insurance products of services" from them. *Id.* ¶ 100.

C. Class Allegations

In the consolidated action, the consolidated Plaintiffs bring their claims on behalf of a nationwide class defined as:

> All United States residents whose PII and/or PHI was accessed or acquired during the ransomware event that is the subject of the Notice of Data Breach that Defendants sent to Plaintiffs and other Class Members on or around August 17, 2021 (the 'Nationwide Class').

CC ¶ 276. In the alternative, the consolidated Plaintiffs seek to represent themselves and nine subclasses (California, Colorado, Florida, Georgia, Illinois, Louisiana, Maryland, New Hampshire, and West Virginia). *Id.* ¶¶ 277–85. Plaintiff May seeks to represent a class of California residents. MC ¶ 66.

The consolidated amended complaint brings claims for: negligence (Count I); breach of implied contract (Count II); unjust enrichment (Count III); violation of

California's Consumer Privacy Act (CCPA) (Count IV); violation of California's Consumers Legal Remedies Act (CLRA) (Count V); violation of California's Customer Records Act (CCRA) (Count VI); violation of California's Confidentiality of Medical Information Act (CMIA) (Count VII); violation of California's Unfair Competition Law (UCL) (Counts VIII and IX); violations of the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA) (Count X); violation of the Louisiana Database Security Breach Notification Law (Count XI); violations of the Maryland Consumer Protection Act (MCPA) (Count XII); violation of the Maryland Personal Information Protection Act (Count XIII); violation of the New Hampshire Consumer Protection Act (NHCPA) (Count XIV); violation of the New Hampshire Notice of Security Breach statute (Count XV); violation of Colorado's Data Security Laws (Count XVI); violation of Colorado's Security Breach Notification Laws (Count XVII); and invasion of privacy (Count XVIII). In their opposition brief to Defendants' motion to dismiss, Plaintiffs voluntarily dismissed their CLRA claim in Count V of the consolidated complaint. [17] at 32 n.9.

The May complaint alleges: violation of the CCPA (Count I); violation of the UCL (Count II); and breach of express contract (Count III). May seeks to represent a class of "[a]ll California residents who Defendants and/or its agents sent a 'Notice of Data Breach' letter to informing them their personally identifiable information (PII) was subjected to the Data Breach." MC ¶ 66.

II. Legal Standard

A motion to dismiss tests the sufficiency of a claim, not the merits of the case. *Gociman v. Loyola Univ. of Chi.*, 41 F.4th 873, 885 (7th Cir. 2022); *Gunn v. Cont'l Cas. Co.*, 968 F.3d 802, 806 (7th Cir. 2020). To survive a motion to dismiss under Rule 12(b)(6), the claim "must provide enough factual information to state a claim to relief that is plausible on its face and raise a right to relief above the speculative level." *Haywood v. Massage Envy Franchising, LLC*, 887 F.3d 329, 333 (7th Cir. 2018) (quoting *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014)); *see also* Fed. R. Civ. P. 8(a)(2) (requiring a complaint to contain a "short and plain statement of the claim showing that the pleader is entitled to relief"). A court deciding a Rule 12(b)(6) motion accepts the well-pleaded factual allegations as true and draws all reasonable inferences in the pleading party's favor. *Lax v. Mayorkas*, 20 F.4th 1178, 1181 (7th Cir. 2021).

Dismissal for failure to state a claim is proper "when the allegations in a complaint, however true, could not raise a claim of entitlement to relief." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007). Deciding the plausibility of the claim is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Bilek v. Fed. Ins. Co.*, 8 F.4th 581, 586–87 (7th Cir. 2021) (quoting *W. Bend Mut. Ins. Co. v. Schumacher*, 844 F.3d 670, 676 (7th Cir. 2016)).

III. Analysis

A. Legal Duty

Defendants first argue that Plaintiffs do not plausibly allege breach of an applicable duty of care, warranting dismissal of Counts I–X, XII–XIV, and XVI of the consolidated complaint. [3] at 19. Defendants argue that all of those counts—which allege negligence, breach of implied contract, statutory data privacy laws, and statutory unfair competition—require Plaintiffs to plead that Defendants fell short of some "reasonable" level of security and that Plaintiffs have failed to do so here. *Id.* at 20. Initially, Defendants improperly presume, without discussing or citing to proper authorities, that these claims require Plaintiffs to plead a "breach of a cognizable duty of care." *See id.* As Plaintiffs point out, the duty of care in the negligence context, which depends on principles of foreseeability and likelihood of injury, is quite different than a contractual breach of contract, which arises from contractual promises the parties made to each other. *Compare, e.g.*, *Hankins v. Alpha Kappa Alpha Sorority, Inc.*, 447 F. Supp. 3d 672, 680 (N.D. Ill. 2020) (discussing the factors that courts analyze to determine whether a legal duty exists in the negligence context) *with Allscripts Healthcare, LLC v. Etransmedia Tech., Inc.*, 448 F. Supp. 3d 898, 904 (N.D. Ill. 2019) ("A breach of contract claim requires . . . the existence of a valid and enforceable contractual promise") (quoting *Doe v. Columbia Coll. Chi.*, 933 F.3d 849, 858 (7th Cir. 2019)). Thus, Defendants' overbroad arguments regarding "breach of a legal duty," which are perfunctory and undeveloped, fail to supply a basis for dismissal. *Crespo v. Colvin*, 824 F.3d 667, 674 (7th Cir. 2016) (quoting *United*

States v. Berkowitz, 927 F.2d 1376, 1384 (7th Cir. 1991)).

Defendants' reliance on *Kuhns v. Scottrade, Inc.* is misplaced. In *Kuhns*, the Eighth Circuit affirmed the dismissal of a breach of implied contract claim in a data breach case because the plaintiff asserted, in conclusory terms, that the defendant failed to take reasonable measures to protect the data. 868 F.3d 711, 718 (8th Cir. 2017). The Eighth Circuit reasoned that the court was "left to guess" how Defendant failed to take security measures. *Id. Kuhns* does not discuss the applicability of a legal duty, as Defendants argue. Moreover, *Kuhns* is distinguishable to the extent Defendants use it to argue that Plaintiffs have failed to plead sufficient facts regarding the types of reasonable security measures Defendants should have taken. Here, in contrast to *Kuhns*, Plaintiffs have alleged that: (1) the United States government recommends certain measures that organizations can take to prevent and detect ransomware attacks, including awareness and training programs, spam filters, firewalls, anti-virus and anti-malware programs; and (2) Defendants failed to implement "one or more of the above measures to prevent ransomware attacks." CC ¶¶ 62, 66. This sufficiently identifies the measures Defendants allegedly fell short of implementing, demonstrating that Plaintiffs have sufficiently alleged a breach for purposes of the negligence claim at this pleading stage.

B. Causation

Defendants argue that fourteen of Plaintiffs' claims (Counts I, II, V–VI, VIII–V, XVII–XVIII) in the consolidated complaint must be dismissed because Plaintiffs do not plausibly plead that Defendants caused them harm. [3] at 22. As with their

"breach of legal duty" argument above, Defendants advocate for a blanket dismissal of these claims, without parsing each legal theory or setting forth the appropriate authorities demonstrating why these claims require dismissal.

In any event, this argument is unpersuasive. Defendants argue that Plaintiffs allege harms that could *not* have been caused by the Data Breach, pointing to, for example, the fact that twelve Plaintiffs allege an increase in spam calls, emails and texts but none allege that their phone numbers or email addresses were compromised. [3] at 23 (citing CC ¶¶ 99, 106, 133, 134, 146, 153, 158, 159, 170, 173, 183, 196, 202, 209, 214, 220, 224, 227, 238, 240, 251, 254, 266, 273). To be sure, it strains plausibility to assume that Defendants caused increased spam to those Plaintiffs who do not allege that their contact information was accessed via the Data Breach. Nevertheless, Plaintiffs plausibly allege that the Data Breach caused other types of harm. For instance, all of these Plaintiffs allege "lost time," anxiety, and increased concerns for the loss of the privacy as a result of the Data Breach. CC ¶ 100, 104, 112, 116, 123, 127, 136, 140, 147, 151, 164, 177, 184, 188, 203, 207, 215, 219, 228, 232, 241, 245, 260.

C. Damages

Defendants argue that nine of the named Plaintiffs in the consolidated complaint—Caswell, Kroll, Horning, Owens, Mitchell, Myers, Parsons, Villalobos, and Wellikoff—fail to allege cognizable damages, warranting dismissal of the following claims: (1) negligence, (2) breach of implied contract, (3) CLRA; (4) UCL;

(5) CCRA, (6) ICFA; (7) LDSBNA; (8) MCPA; (9) NHCPA; and (10) New Hampshire Notice of Security Breach statute. [3] at 24.

Once again, Defendants generalize that many of Plaintiffs' claims require pleading of actual, pecuniary harm, without accounting for critical differences in pleading each cause of action. This Court's own research has revealed that the pleading requirements for each claim can differ, and thus will walk through each claim one by one.

First, Illinois law[2] requires a plaintiff to plead a "legally cognizable present injury or damage to sustain a negligence claim." *Leslie v. Medline Indus., Inc.*, No. 20-CV-01654, 2021 WL 4477923, at *7 (N.D. Ill. Sept. 30, 2021) (quoting *Yu v. Int'l Bus. Machs. Corp.*, 732 N.E.2d 1173, 1177 (Ill. App. Ct. 2000)). There can be no dispute that Plaintiffs have alleged present injuries or damages; for instance, all allege experiencing emotional harms such as anxiety and increased concerns for the loss of privacy. *See, e.g.*, CC ¶ 219. These types of non-economic damages are recoverable under Illinois law. *See Volling v. Antioch Rescue Squad*, 999 F. Supp. 2d 991, 999 (N.D. Ill. 2013); *see also Epping v. Commonwealth Edison Co.*, 734 N.E.2d 916, 920 (Ill. App. Ct. 2000).

To plead a viable breach of implied contract claim under Illinois law,[3] Plaintiffs must allege "actual monetary damage." *Moyer v. Michaels Stores, Inc.*, No.

[2] This Court applies Illinois law because the parties raise no choice of law conflict. *See Sosa v. Onfido, Inc.*, 8 F.4th 631, 637 (7th Cir. 2021) (explaining that under Illinois choice of law rules, courts apply forum law unless a party demonstrates an actual conflict with another state's law or the parties agree that another state's law applies).

[3] Again, because neither party raises a choice of law conflict, the Court presumes that Illinois law applies. *See, e.g.*, *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 764–65 (C.D. Ill. 2020) (applying Illinois

14 C 561, 2014 WL 3511500, at *7 (N.D. Ill. July 14, 2014); *see also Archey v. Osmose Utilities Servs., Inc.*, No. 20-CV-05247, 2021 WL 3367156, at *2 (N.D. Ill. Aug. 3, 2021). Some Plaintiffs have alleged concrete monetary losses. Plaintiff Kroll alleges the loss of the economic value of purchases she would have made but for the Data Breach. Plaintiff Owens spent $100.00 purchasing a spam blocker due to the alleged increase in spam calls due to the Data Breach. CC ¶ 220. Moreover, all of the Plaintiffs have alleged injury in the form of time lost dealing with the consequences of the Data Breach, including verifying the accuracy of the notices they received and self-monitoring their accounts. *See* CC ¶¶ 99, 112, 123, 136, 147, 160, 171, 184, 203, 215, 228, 241, 256. Although neither party has pointed to Illinois cases discussing the scope of recoverable "actual monetary damage" in the context of implied contract cases, the Seventh Circuit has remarked in a data breach case that generally "the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective. These injuries *can justify money damages*, just as they support standing." *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018) (emphasis added). Because all Plaintiffs plead some type of lost time, they have sufficiently pled economic injuries for the purposes of their implied contract claim.

To survive a motion to dismiss an ICFA claim, a plaintiff must allege actual pecuniary loss. *Id.* at 887 F.3d 826, 829–30; *see also Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739 (7th Cir. 2014) (explaining that a private ICFA plaintiff must allege actual pecuniary loss). Kroll, the named Plaintiff on the ICFA

law to breach of contract claim because "Plaintiffs have not claimed the existence of an outcome determinative conflict").

claim, sufficiently alleges economic injury within the meaning of the ICFA. Kroll alleges that she experienced fraudulent charges on her credit card which rendered her unable to purchase furniture. CC ¶ 159. This represents lost economic value. She also alleges that she still experiences difficulty today when she attempts to make larger purchases on her credit card due to the prior fraudulent charges. *Id.* Kroll's inability to make certain purchases constitutes an economic injury which remains viable under the ICFA.

The California Plaintiffs[4] adequately allege damages under the California consumer protection statutes. The California UCL provides that "lost money or property" supports recovery, and California courts hold that "lost money or property" means "economic injury." *Dieffenbach*, 887 F.3d at 829 (first quoting Cal. Bus. & Prof. Code § 17204; then citing *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011)). All California Plaintiffs have alleged expending significant time incurred to contend with the Data Breach, and California courts consider "time lost" to constitute economic injury. *Dieffenbach*, 887 F.3d at 829 (observing that California "state courts have said that significant time and paperwork costs incurred to rectify violations also can qualify as economic losses"); *see* CC ¶¶ 112, 136, 171, 184, 256. The same analysis applies to the California Plaintiffs' claim under the CCRA, which provides that a "customer injured by a violation of [this Act] may . . . recover damages." Cal. Civ. Code § 1798.84. Neither statute nor any state decision defines "injury." *Dieffenbach*, 887 F.3d at 829. But even if a CRA "injury" requires an

[4] The consolidated complaint defines "California Plaintiffs" as including Plaintiffs Villalobos, Davie, Marr, McDonald, and Yeremian. CC ¶ 277.

economic loss, as discussed above, the California Plaintiffs have alleged such losses. *See id.* (holding that even if a CCRA injury required economic injury, like the UCL, the plaintiffs had met their pleading burden).

As for Plaintiff Parsons, his claim under the Louisiana Database Security Breach Notification Law (LDSBNL) requires him to plead "actual damages." *Pinero v. Jackson Hewitt Tax Serv. Inc.*, 594 F. Supp. 2d 710, 716 (E.D. La. 2009) (quoting La. Rev. Stat. 51:3075). A Louisiana federal court interpreting Louisiana law construed the term "actual damages" narrowly, meaning that the plaintiff must allege that someone "actually used the disclosed information to his detriment." *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 798 (M.D. La. 2007). In other words, it is not enough to merely complain about the "current burden" of monitoring credit, scrutinizing account statements, and closing and opening accounts. *Id.* Based on this authority, Parsons has not adequately stated a claim for actual damages under the LDSBNL. He alleges only that he suffers "imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse" of his PII and PHI, not that a third party actually used his information to his detriment. For this reason, this Court dismisses Parsons' LDSBNL claim in Count XI.

Next, Maryland courts have held that the MCPA requires plaintiffs to have suffered an "objectively identifiable loss," as "measured by the amount the consumer spent or lost." *Attias v. CareFirst, Inc.*, 518 F. Supp. 3d 43, 56 (D.D.C. 2021) (quoting *Lloyd v. Gen. Motors Corp.*, 397 Md. 108, 916 A.2d 257, 277 (Md. 2007)); *see also Ayres v. Ocwen Loan Servicing, LLC*, 129 F. Supp. 3d 249, 270 (D. Md. 2015).

Cognizable losses include emotional damages or mental anguish. *See Ayres*, 129 F. Supp. 3d. at 270 (collecting cases). Both Maryland Plaintiffs, Owens and Welikoff, allege annoyance, interference, inconvenience, anxiety, and increased concerns for the loss of their families' privacy. CC ¶¶ 219, 232. Thus, they have sufficiently alleged damages under the MCPA.

Finally, the New Hampshire Consumer Protection Act (NHCPA) requires "that the Plaintiffs show that the class members were personally harmed in some way by the Defendant's unlawful conduct." *Pagan v. Abbott Lab'ys, Inc.*, 287 F.R.D. 139, 149 (E.D.N.Y. 2012). Mitchell, the named Plaintiff on the NHCPA claim, claims to have suffered emotional harm and time lost, among other things. CC ¶¶ 203, 207. Defendants have presented no authority suggesting that these harms are not cognizable under the NHCPA, and this Court has found none. Thus, this Court declines to dismiss the NHCPA claim due to failure to plead damages.

D. Data Breach Notification Statutes

Defendants argue that Plaintiffs' notification statute claims (Counts VI, X, XI, XIII, XV, and XVII of the consolidated complaint) fail to allege cognizable harm which in this context means damages or incremental injury from Defendants' delay in notifying Plaintiffs of the Data Breach. [3] at 29.

The data breach notification statutes all require companies to notify individuals of data breaches without unreasonable delay. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1149 (C.D. Cal. 2021) (observing that the CCRA requires businesses doing business in California to make disclosure of data

breaches "in the most expedient time possible and without unreasonable delay") (quoting Cal. Civ. Code § 1798.82); 815 Ill. Comp. Stat. 530/10(a) (setting forth Illinois' requirement to provide a "disclosure notification . . . in the most expedient time possible and without unreasonable delay")[5]; La. Stat. Ann. § 51:3074(E) (requiring notification "in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach"); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 487 (D. Md. 2020) (explaining that the Maryland law requires notification be "given as soon as reasonably practical after the business discovers or is notified of the breach of a security system") (quoting Md. Comm. Code §§ 14-3504(b)(2), 14-3504(c)(2)); N.H. Rev. Stat. Ann. § 359-C:20(1)(A) (requiring disclosure "as soon as possible"); Colo. Rev. Stat. Ann. § 6-1-716(2) ("Notice must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred.").

In moving to dismiss these claims, Defendants argue that Plaintiffs have not alleged incremental harm as a result of the delayed notification, as opposed to harm from the Data Breach generally. Not so. Plaintiffs allege that Defendants began notifying some class members of the Data Breach on June 30, 2021, more than nine months after reports began surfacing on the internet about the data breach. CC ¶ 8.

[5] As part of her ICFA claim, Kroll alleges that Defendants violated the Illinois Personal Information Protection Act (PIPA) by failing to immediately notify Plaintiff and the Illinois class. CC ¶ 423. A "violation of the PIPA can be sufficient to obtain ICFA relief." *Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 824 (7th Cir. 2018).

A nine-month delay is sufficient to raise an inference that the delay was "unreasonable." *See, e.g.*, *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-CV-2284-H-KSC, 2020 WL 2214152, at *14 (S.D. Cal. May 7, 2020) (inferring that a five-month delay in notification was unreasonable). Plaintiffs also allege that the delayed notice prevented them from timely mitigating, preventing, and repairing identity theft and the fraudulent use of their PII and/or PHI by third parties, CC ¶¶ 315, 481. This establishes, for pleading purposes, that Plaintiffs suffered harm from the delay in notification. *See, e.g.*, *Solara*, 2020 WL 2214152, at *14 (holding that the plaintiff adequately alleged harm from unreasonable delay in notification by stating that the "delay prevented him from taking steps to protect his personal information from identify theft"). Moreover, allegations of Plaintiffs' post-disclosure remedial actions—coupled with allegations of harm by the Data Breach itself—raise an inference that "timely disclosure would have prompted a swifter response and that the delay caused . . . cognizable injury." *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, No. 21-MD-02994-RAR, 2022 WL 1468057, at *21 (S.D. Fla. May 10, 2022) (analyzing whether the plaintiff adequately pled a CCRA claim). Here, Plaintiffs have all alleged post-remedial actions and harm from the Data Breach, making it plausible to conclude that Defendants' more timely disclosure would have prevented additional incremental injury. For these reasons, this Court will not dismiss the data notification statutes for failure to alleged incremental harm from any delay in notification.

E. Plaintiffs' Relationships to Defendants

Defendants contend that Plaintiffs' "attenuated" relationships with Defendants foreclose their negligence, implied contract, and unjust enrichment claims in Counts I–IIII of the consolidated complaint. The Court turns to each claim in order below.

1. Negligence

Defendants first argue that Plaintiffs' negligence claim requires the Court to predict that the law recognizes a "common law data security duty," and the Seventh Circuit predicted in *Community Bank of Trenton v. Schnuck Markets, Inc.* that the Illinois Supreme Court "would not impose" a common law data security duty. See [3] at 30 (citing 887 F.3d 803, 816 (7th Cir. 2018)). *Schnuck* relied on the Illinois appellate court's opinion in *Cooney v. Chicago Public Schools*, 943 N.E.2d 23, 28 (2010), which rejected the notion of a "new common law duty" to safeguard information. *Schnuck*, 887 F.3d at 816. But the Illinois appellate court decided *Cooney* before the Illinois legislature's amendment of PIPA in 2017; that amendment now requires data collectors to "implement and maintain reasonable security measures to protect" records from "unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 Ill. Comp. Stat. § 530/45(a); *see* [3] at 30. As Defendants concede, this amendment calls into question the continued viability of *Schnuck*'s holding that there exists no duty under Illinois law to safeguard personal information. This Court therefore declines at this stage of the proceedings to dismiss based on the non-existence of a data security duty under Illinois law.

2. Breach of Implied Contract

Defendants also move for dismissal of the implied contract claim, arguing that Plaintiffs allege no conduct from which a contract could be implied against Defendants. [3] at 30. In Illinois, the elements of a breach of implied contract claim track those of a breach of express contract claim; a plaintiff must allege: (1) the existence of a valid and enforceable contract; (2) performance by the plaintiff; (3) breach of contract by the defendant; and (4) resultant injury to the plaintiff. *Archey v. Osmose Utilities Servs., Inc.*, No. 20-CV-05247, 2022 WL 3543469, at *2 (N.D. Ill. Aug. 18, 2022) (citing *Hess v. Bresney*, 784 F.3d 1154, 1158–59 (7th Cir. 2015)). An implied contract arises from a "promissory expression which may be inferred from the facts and circumstances and the expressions [on] the part of the promisor which show an intention to be bound." *Doe v. Fertility Centers of Ill., S.C.*, No. 21 C 579, 2022 WL 972295, at *4 (N.D. Ill. Mar. 31, 2022) (alteration in original) (quoting *Estate of Jesmer v. Rohlev,* 609 N.E.2d 816, 820 (Ill. App. Ct. 1993)). Of course, there must also be a "meeting of the minds or mutual assent as to the terms of the contract." *Nw. Mem'l Healthcare v. Anthem Ins. Companies, Inc.*, No. 21 C 6306, 2022 WL 1620025, at *2 (N.D. Ill. May 23, 2022) (quoting *Dynegy Mktg. & Trade v. Multiut Corp.*, 648 F.3d 506, 515 (7th Cir. 2011)).

The consolidated complaint reveals that the majority of the Plaintiffs could not have reached a "meeting of the minds" with Defendants. Among the Plaintiffs, only Parsons and Yeremian worked for one of the Defendants. CC ¶¶ 96, 248. 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. *See, e.g.*, *Doe*, 2022 WL 972295, at *4 (dismissing implied contract claim in a data breach case where the plaintiff was unaware of the company whose data breach allegedly caused disclosure of the plaintiff's sensitive medical information).

Defendants also contend that the Plaintiffs with direct employment relationships with Defendants—Parsons and Yeremian—also fail to state viable implied contract claims because they do not allege facts showing mutual assent for the protection of Plaintiffs' PII and PHI. [3] at 31–32. But courts "that have found an implied contract in the employee-employer data breach context have done so when the plaintiffs were able to point to some document, expression, or action of the employer which indicated an intention to protect the employee's personal information." *Archey v. Osmose Utilities Servs., Inc.*, No. 20-CV-05247, 2022 WL 3543469, at *4 (N.D. Ill. Aug. 18, 2022). And here, Plaintiffs have pled the existence of Defendants' privacy policy which applied to personal information collected from individuals and represents that Defendant would "restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes." CC ¶¶ 52–53. This policy supports a finding of an implicit promise to protect employees' personal information in exchange for their employment. *See, e.g.*, *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 750 (S.D.N.Y. 2017) ("TransPerfect's privacy policies and security practices manual—which states that the company 'maintains robust procedures designed to carefully

protect the PII with which it [is] entrusted'—further supports a finding of an implicit promise" under New York law).

Thus, Parsons and Yeremian remain as Plaintiffs asserting the implied contract claim in Count II. This Court dismisses the remaining Plaintiffs from Count II of the consolidated complaint.

3. Unjust Enrichment

Defendants argue that Plaintiffs' unjust enrichment must be dismissed because they fail to allege that Defendants retained any benefit. [3] at 32–33. This Court agrees. To survive a motion to dismiss an unjust enrichment claim, Plaintiffs must plausibly allege that Defendants unjustly retained a benefit, resulting in a detriment to Plaintiffs. *See, e.g.*, *Buschauer v. Columbia Coll. Chi.*, No. 20 C 3394, 2022 WL 103695, at *3 (N.D. Ill. Jan. 10, 2022) (citing *HPI Health Care Servs. v. Mt. Vernon Hosp.*, 545 N.E.2d 672 (Ill. 1989)), *appeal dismissed*, No. 22-1216, 2022 WL 3211433 (7th Cir. Apr. 7, 2022); *see* [17] at 31 (agreeing with Defendants that unjust enrichment requires the defendant's retention of a benefit).

Plaintiffs have not plausibly alleged Defendants' retention of a benefit conferred by Plaintiffs. If anything, the consolidated amended complaint suggests that third-party hackers, not Defendants, are the ones who benefitted from the Data Breach. Plaintiffs insist that Defendants retained the "monetary benefit" of Plaintiffs' "valuable PII and PHI." CC ¶ 343. Courts have, however, routinely rejected the "proposition that an individual's personal identifying information has an independent monetary value." *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d

735, 755 (W.D.N.Y. 2017) (quoting *Welborn v. Internal Revenue Serv.*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016)); *see also, e.g.*, *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (finding no Article III standing from such an "abstract injury" in the "loss of [plaintiffs'] private information"). For this reason, this Court dismisses Plaintiffs' unjust enrichment claim in Count III.

F. California Claims

This Court will now address Defendants' arguments regarding the sufficiency of the claims brought by the various Plaintiffs under California statutes.

1. CCPA Claims

Defendants move to dismiss Count IV of the consolidated complaint arguing that Myers, the lone named Plaintiff, fails to adequately allege a violation of the California Consumer Privacy Act (CCPA). [3] at 33–35. The CCPA provides: "Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action." Cal. Civ. Code § 1798.150(a)(1).

This Court agrees that Myers' CCPA claim is deficient because, as both parties acknowledge, Plaintiffs' counsel inadvertently omitted allegations regarding Myers' personal experience with the Data Breach, including his relationship with Defendants and how the Data Breach injured him specifically. *See generally* CC. Plaintiffs have requested leave to amend to include these allegations, [17] at 33 n.10,

and this Court will grant that request. Because Myers will be amending the CCPA claim, this Court declines at this time to address Defendants' other arguments on that claim. In addition, this Court notes that the consolidated complaint does not name Myers as one of the "California Plaintiffs." *See* CC ¶ 277. This Court thus assumes that Myers does not purport to bring the claims asserted on behalf of the California Plaintiffs—Counts VI (CCRA), VII (CMIA), and VIII–IX (UCL).

Defendants also move to dismiss Count I of the May complaint, which alleges a violation of the CCPA. MC ¶¶ 75–86. Specifically, Defendants argue that May fails to allege a specific action Defendants took or failed to take that breached a duty under the CCPA to maintain "reasonable" security measures. [5] at 6. But they cite no authority requiring such specificity at this stage of the proceedings. This Court finds it sufficient that May alleges a Data Breach caused by Defendants' purported lack of reasonable security measures that allowed third parties to view and steal her personal information. *See, e.g.*, *Mehta v. Robinhood Fin. LLC*, No. 21-CV-01013-SVK, 2021 WL 6882377, at *8 (N.D. Cal. May 6, 2021) (denying motion to dismiss CCPA claim based on allegations that the defendants violated their duty to maintain reasonable security measures by "allow[ing] unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted personal information of Plaintiffs and other customers, including their personal and financial information").

Defendants also argue that May inadequately alleges that she is a "customer," and that Defendants constitute "businesses," under the CCPA. This argument fares

no better. The CCPA defines "consumer" broadly as a "natural person who is a California resident," Cal. Civ. Code § 1798.140(g), and May is a California resident, MC ¶ 7. Moreover, the May complaint plausibly alleges that Defendants meet the definition of "businesses" under the CCPA. The CCPA allows consumer actions to redress a "*business*'s violation of the duty to implement and maintain reasonable security procedures and practices." Cal. Civ. Code § 1798.150(a)(1) (emphasis added). Under the CCPA, "business" means an entity "that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information." Cal. Civ. Code § 1798.140(c)(1). The May complaint sufficiently alleges that Defendants are "businesses" because, according to May, they collected her personal information. *See, e.g.*, *Karter v. Epiq Sys., Inc.*, No. SACV2001385CJCKESX, 2021 WL 4353274, at *2 (C.D. Cal. July 16, 2021) (finding that a complaint adequately alleged that the defendant was a "business" because in order to perform its service, "which it performs pursuant to contracts with other entities," the defendant allegedly collected consumers' personal information); MC ¶ 11. For these reasons, this Court denies Defendants' motion to dismiss Count I of the May complaint.

2. CCRA Claim

Defendants move for dismissal of the CCRA claim in Count VI, which California Plaintiffs (Villalobos, Davie, Marr, McDonald, and Yeremian) bring on behalf of a putative California subclass. [3] at 39–40; CC ¶¶ 277, Count VI.

Defendants argue that the California Plaintiffs are not "customers," as defined under the CCRA, and thus lack statutory standing to bring a claim.

The CCRA "regulates businesses with regard to treatment and notification procedures relating to their customers' personal information." *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1142 (N.D. Cal. 2018) (quoting *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600-RGK, 2015 WL 3916744, at *6 (C.D. Cal. June 15, 2015)). The statute limits civil actions to "any customer," defined 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." Cal. Civ. Code §§ 1798.80(c); 1798.84.

Based on this definition, the Court agrees with Defendants that two of the California Plaintiffs do not meet the definition of "customer" under the CRA. Plaintiff Yeremian provided her PII and PHI to Defendants in the course of her employment with AJG, not for the purpose of obtaining a service or a product. CC ¶ 249; *see Corona*, 2015 WL 3916744, at *7 (holding that former employees of the defendant were not "customers" under the CRA where they provided their personal data to defendant in the course of their employment). Villalobos, another one of the California Plaintiffs, does not know how his PII and/or PHI became compromised during the Data Breach; he pleads only that he entrusted his PII and/or PHI to Defendants, "possibly through a third-party that provided human resources services to Prolacta." CC ¶ 109. This is insufficient to show that Villalobos provided his information "for the purpose of purchasing or leasing a product or obtaining a

service." Cal. Civ. Code § 1798.80(c). Thus, this Court dismisses Yeremian and Villalobos from the CCRA claim in Count VI.

The remaining California Plaintiffs plausibly plead that they constitute "customers" under the CCRA. Davie alleges that he entrusted his PII and/or PHI to GBS "as the third-party administrator" for his employer, Whirlpool's, worker compensation claims. CC ¶ 131. Likewise, Marr asserts she provided her PII and/or PHI to one of the Defendants "when she filed a workers' compensation claim for an on-the-job injury" she sustained while working for her employer. CC ¶ 169. McDonald, too, states that he provided his PII and PHI to one of the Defendants as administrator of his employer's workers' compensation insurance. CC ¶ 181. Taking these allegations as true, Davie, Marr, and McDonald all allege that they provided their personal information for the purpose of "obtaining a service," Cal. Civ. Code § 1798.80(c), therein qualifying as "customers" under the CCRA. This Court thus denies the motion to dismiss Davie, Marr, and McDonald from Count VI.

3. CMIA Claim

The CMIA "is intended to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider, while at the same time setting forth limited circumstances in which the release of such information to specified entities or individuals is permissible." *Erhart v. BofI Holding, Inc.*, 269 F. Supp. 3d 1059, 1078 (S.D. Cal. 2017) (quoting *Brown v. Mortensen*, 253 P.3d 522, 533 (Cal. 2011)). To further that end, the CMIA contains a series of provisions regarding the use and disclosure of medical information by

employers. *Id.* (citing Cal. Civ. Code §§ 56.20–56.245). Plaintiff alleges that Defendants violated: (1) CMIA provisions barring disclosure of medical information without prior authorization under the California Civil Code Sections 56.10, 56.11, 56.13, and 56.26; and (2) CMIA provisions forbidding negligent storage of medical information under Section 56.101 and 56.06. CC ¶¶ 397, 400.

Defendants raise several arguments in support of dismissal of the CMIA claim. [3] at 40–43. Dispositive here, Defendants point out that they do not qualify as covered entities under the CMIA. *Id.* at 41. Indeed, for several of the CMIA sections under which the California Plaintiffs seek relief, they must sufficiently allege that Defendants constitute "providers of health care." Under Section 56.10 of the CMIA, a "*provider of health care*, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization, except as provided in subdivision (b) or (c)." Cal. Civ. Code § 56.10(a) (emphasis added). Section 56.11 then sets out the requirements for a obtaining a valid authorization under Section 56.10, *see Colleen M. v. Fertility & Surgical Assocs. of Thousand Oaks*, 34 Cal. Rptr. 3d 439, 442 (Cal. Ct. App. 2005) (citing Cal. Civ. Code § 56.11), and Section 56.13 provides that a recipient of medical information via authorization "may not disclose that medical information" further without additional authorization that meets the requirements of Section 56.11, Cal. Civ. Code § 56.13. Similarly, under Section 56.101 of the CMIA, a "*provider of health care*, health care service plan, pharmaceutical company, or contractor who negligently

creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Cal. Civ. Code § 56.101 (emphasis added).

Beyond their conclusory allegation that Defendants "were healthcare providers for the purposes of this cause of action," CC ¶ 389, the consolidated complaint makes clear that the Defendants do not meet the definition of "provider of healthcare." Under the Civil Code, a "provider of health care" means:

> a person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code; a person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act; a person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code; or a clinic, health dispensary, or health facility licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code. "Provider of health care" does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code.

Cal. Civ. Code § 56.05(m). Defendant AJG is an insurance brokerage, risk management, and HR & benefits consulting company; GBS is a third-party administrator and claims manager. CC ¶¶ 2–3. They are not "providers of healthcare" under the statute.

To be sure, as Plaintiff points out, the CMIA provides that, in addition to traditional medical providers, a "provider of healthcare" includes any "business organized for the purpose of maintaining medical information." *Oddei v. Optum, Inc.*, No. 2:21-CV-03974-SB-MRW, 2021 WL 6333467, at *2 (C.D. Cal. Dec. 3, 2021) (quoting Cal. Civ. Code § 56.06(a)–(b)); *see* [17] at 38–39. But the consolidated complaint alleges merely that Defendants maintain medical information; it is

otherwise devoid of any allegation that either Defendant is organized *for the purpose* of maintaining medical information. Thus, the California Plaintiffs fail to allege that Defendants constitute "providers of healthcare" subject to Sections 56.10, 56.11, 56.13, 56.101, and 56.101 of the CMIA.

The California Plaintiffs also assert that Defendants violated Section 56.26 of the CMIA, which provides:

> No person or entity engaged in the *business of furnishing administrative services to programs that provide payment for health care services* shall *knowingly* use, disclose, or permit its employees or agents to use or disclose medical information possessed in connection with performing administrative functions for a program, except as reasonably necessary in connection with the administration or maintenance of the program, or as required by law, or with an authorization.

Cal. Civ. Code § 56.26(a) (emphasis added); *see* CC ¶ 397. But Section 56.26 is inapplicable, too. The consolidated complaint contains no allegation suggesting that either Defendant is in the business of furnishing administrative services to programs that provide payment for health care services. Nor does the consolidated complaint suggest any "knowing" disclosure of medical information to an unauthorized individual.

For these reasons, this Court dismisses the CMIA claim in Count VII of the consolidated complaint.

4. UCL Claims

Defendants move for dismissal of the UCL claims in Counts VIII and IX of the consolidated complaint and Count II of the May complaint. Count VIII (brought only on behalf of California Plaintiffs) of the consolidated complaint asserts unlawful

business practices, and Count IX (brought on behalf of all Plaintiffs, or alternatively, the California Plaintiffs) asserts unfair business practices. Count II of the May complaint alleges that Defendants engaged in unlawful, unfair, and fraudulent business practices.

The UCL serves the purpose of preserving "fair competition" and protects consumers from "market distortions." *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 331 (2011). The UCL prohibits an individual or entity from engaging in any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Each UCL prong constitutes a separate and distinct theory of liability. *Ginsberg v. Google Inc.*, No. 21-CV-00570-BLF, 2022 WL 504166, at *6 (N.D. Cal. Feb. 18, 2022) (citing *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959 (9th Cir. 2009)). Defendants advance a host of arguments in support of dismissal, but only one is dispositive here: California law does not permit extra-territorial application of the UCL under the circumstances of this case.

Under California's presumption against extra-territoriality, ordinarily "the statutes of a state have no force beyond its boundaries." *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018) (quoting *N. Alaska Salmon Co. v. Pillsbury*, 162 P. 93, 94 (Cal. 1916)). The key test looks at whether the conduct creating liability occurs in California: if the "conduct that 'creates liability' occurs in California, California law properly governs that conduct," but "if the liability-creating conduct occurs outside of California, California law generally should not govern that conduct" unless the legislature indicates otherwise. *Id.* (first quoting *Sullivan v. Oracle Corp.*,

254 P.3d 237, 248 (Cal 2011); then citing *Diamond Multimedia Sys., Inc. v. Superior Court*, 968 P.2d 539, 554 (Cal. 1999)). The California Supreme Court has instructed that California's presumption against extraterritoriality applies to the UCL "in full force." *Sullivan*, 254 P.3d at 248.

Here, Defendants are Delaware corporations who maintain their principal places of business in Illinois. CC ¶¶ 42, 43. Plaintiffs do not allege that the Defendants' wrongful conduct—implementing poor security measures—emanated from California. Rather, they suggest that the Data Breach stemmed from a ransomware attack to Defendants' internal servers—presumably located at their headquarters in Illinois. *E.g.*, CC ¶ 55. The conduct "allegedly creating liability in this case occurred wholly outside of California." *Toretto v. Donnelley Fin. Sols., Inc.*, No. 1:20-CV-2667-GHW, 2022 WL 348412, at *20 (S.D.N.Y. Feb. 4, 2022) (dismissing UCL claim brought by California resident against non-resident defendants where the alleged wrongdoing occurred outside of California); *see also, e.g.*, *Fernandez v. CoreLogic Credco, LLC.*, No. 320CV1262JMAGS, 2022 WL 891226, at *13 (S.D. Cal. Mar. 25, 2022) (observing that "non-California residents are foreclosed from bringing claims under California's consumer protection laws, such as the UCL, 'where none of the alleged misconduct or injuries occurred in California'") (quoting *Churchill Vill., L.L.C. v. Gen. Elec. Co.*, 169 F. Supp. 2d 1119, 1126 (N.D. Cal. 2000), *aff'd sub nom. Churchill Vill., L.L.C. v. Gen. Elec.*, 361 F.3d 566 (9th Cir. 2004)). This Court dismisses the UCL claims in Counts VIII and IX of the consolidated complaint and Count II of the May complaint.

G. Maryland Personal Information Protection Act

Defendants move to dismiss Count XIII of the consolidated complaint on the basis that the Maryland Personal Information Protection Act (MPIPA) does not supply a private right of action. [3] at 49. The Court grants this request. The MPIPA contains no private right of action; instead, a violation of the MPIPA constitutes "an unfair or deceptive trade practice" "subject to the enforcement and penalty provisions" of the MCPA. *In re Mednax Servs., Inc., Customer Data Sec. Breach Litig.*, No. 21-MD-02994-RAR, 2022 WL 1468057, at *14 (S.D. Fla. May 10, 2022) (quoting Md. Comm. Law § 14-3508). Thus, to the extent the Maryland Plaintiffs seek relief for violations of the MPIPA, they must do so under the MCPA—the claim they already assert in Count XII of the consolidated complaint. *See id.*; *see also Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 27 (D.D.C. 2019) (noting that "consumers may bring a violation of [the MPIPA] as an unfair or deceptive trade practice under the MCPA"). This Court dismisses the standalone MPIPA claim in Count XIII.

H. Colorado Statutes

Like the MPIPA claim, Defendants move to dismiss Counts XVI and XVII of the consolidated complaint, arguing that those counts alleging violations of Colorado statutes do not provide a private right of action. [3] at 49. Again, the Court grants this request. Count XVI purports to plead a violation of Section 6-1-713.5 of the Colorado Revised Statutes, which requires covered entities to "maintain reasonable security procedures and practices" to protect PII. Colo. Rev. Stat. § 6-1-713.5. Count

XVII alleges a violation of Section 6-1-716, which requires notice to Colorado residents affected by a security breach. Colo. Rev. Stat. § 6-1-716.

Neither section, however, supplies a private right of action. Instead, Colorado's code provides that: "The attorney general may bring an action in law or equity to address violations of this section [Section 6-1-716], section 6-1-713, or section 6-1-713.5, and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both." Colo. Rev. Stat. Ann. § 6-1-716; *see also Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, No. 15-CV-02129-MSK-NYW, 2016 WL 8578096, at *12 n.9 (D. Colo. June 20, 2016) (explaining that the Colorado "Data Breach Statutes does not provide for a private right of action"), *report and recommendation adopted*, No. 15-CV-02129-MSK-NYW, 2016 WL 8578252 (D. Colo. Sept. 21, 2016); *Kylie S. v. Pearson PLC*, 475 F. Supp. 3d 841, 850 (N.D. Ill. 2020) (noting that "the Colorado notification law does not create a private right of action").

Plaintiffs rely on *In re Target Corp. Data Security Breach Litigation*, where the district court declined to dismiss a Section 6-1-716 claim. 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014). The court found the language of the statute "permissive," and thus "ambiguous," as to whether a private right of action exists in addition to the attorney general's enforcement powers. *Id.* Respectfully, this Court disagrees with *Target*'s conclusion to retain the Colorado statutory claim. Colorado law requires "a clear expression of legislative intent before installing a private right of action in a statute otherwise silent on the matter." *Sigstedt v. Colorado Mountain Loc. Coll.*

Dist., 550 F. Supp. 3d 928, 932 (D. Colo. 2021) (quoting *City of Arvada ex rel. Arvada Police Dep't v. Denver Health & Hosp. Auth.*, 403 P.3d 609, 614 (Colo. 2017)); *see also Gerrity Oil & Gas Corp. v. Magness*, 946 P.2d 913, 923 (Colo. 1997). There is no clear expression of legislative intent here. Accordingly, this Court concludes that the Colorado code does not provide a private right of action for Plaintiffs' claims. and dismisses the Colorado statutory claims in Counts XVI and XVII of the consolidated complaint.

I. Invasion of Privacy

Defendants move to dismiss Count XVIII of the consolidated complaint, which alleges "invasion" of privacy on behalf of all Plaintiffs. As clarified in their opposition brief, Plaintiffs' invasion of privacy claim arises from a theory of intentional intrusion upon seclusion. [17] at 48; *see also* CC ¶ 506 (alleging that the Data Breach "constitutes an intentional interference with Plaintiffs' . . . interest in solitude or seclusion"). This Court agrees with Defendants that Plaintiffs have failed to adequately plead this claim.

Under Illinois law, a claim of intrusion upon seclusion requires the following elements: (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is highly offensive or objectionable to a reasonable person; (3) that the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering. *Angelo v. Moriarty*, No. 15 C 8065, 2016 WL 640525, at *4 (N.D. Ill. Feb. 18, 2016) (citing *Jacobson v. CBS Broad., Inc.,* 19 N.E.3d 1165 (Ill. App. Ct. 2014)). Plaintiffs' claim is deficient because there is no allegation that

Defendants obtained Plaintiffs' PII and PHI through an "unauthorized intrusion." Instead, the consolidated complaint alleges that Plaintiffs "disclosed their PII and PHI to Defendants as part of their relationships with Defendants." CC ¶ 505. *Bonilla v. Ancestry.com Operations Inc.*, 574 F. Supp. 3d 582, 597 (N.D. Ill. 2021). Plaintiffs' voluntary disclosure of their PII and PHI, either directly to Defendants or indirectly through their employers, dooms their claim. *See, e.g.*, *Bonilla v. Ancestry.com Operations Inc.*, 574 F. Supp. 3d 582, 597 (N.D. Ill. 2021) (dismissing intrusion claim because there "are no allegations that [the defendant]'s collection of [personal information] was unauthorized"). This Court dismisses Plaintiffs' invasion of privacy claim in Count XVIII of the consolidated complaint.

J. Breach of Express Contract: May

Defendants move to dismiss Count III of the May complaint, arguing that she fails to allege the existence or breach of any contract, or any resulting damages. Under California law, which the parties agree applies to this claim, May must allege the following four elements: (1) the existence of the contract, (2) May's performance or excuse for nonperformance, (3) Defendants' breach, and (4) resulting damages. *Oasis W. Realty, LLC v. Goldman*, 250 P.3d 1115, 1121 (Cal. 2011).

Plaintiff's breach of contract theory rests on Defendants' Terms of Use and Privacy Policy which she alleges is the express contract the parties entered into once Plaintiff provided her PII to Defendants "in relation to [her] purchase of insurance products or services" from them. MC ¶ 100. This contract, Plaintiff alleges, includes Defendants' promises to implement certain measures "to help ensure a level of

security appropriate to the risk to the personal information we collect, use, disclosure, and process" and to "restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes." *Id.* ¶¶ 39–40.

Defendants argue that May does not plausibly allege an enforceable contract because she does not state when Defendants offered the Terms of Use and Privacy Policy to May, when or how May accepted the contract, or how the parties exchanged consideration. But the law does not require such specificity. This Court finds it sufficient that May alleges that she was offered and accepted the Terms of Use and Privacy Policy upon purchase of Defendants' services or products. *See, e.g.*, *Solara*, 2020 WL 2214152, at *5 (denying motion to dismissbreach of express contract claim based on similar allegations that the defendant breached a privacy policy). Moreover, the existence of consideration is self-evident from May's allegations: Defendants provided a product or service in exchange for May's payment.

Defendants also unpersuasively argue that May inadequately alleges breach of the contract. They emphasize the complaint's allegations that the Terms of Use and Privacy Policy acknowledge that "no security measures are perfect or impenetrable" as representing a warranty of adequate, but not perfect, security. MC ¶ 39. But May also alleges that the contract contains a promise to restrict "access to your personal information to those who require access to such information for legitimate, relevant business purposes," and that the Data Breach resulted in a breach of this promise. *Id.* ¶¶ 41, 99. This plausibly alleges a breach of the Terms of

Use and Privacy Policy. Finally, this Court also rejects Defendants' contention that May has not adequately alleged contractual damages. In California, the "dissemination of one's personal information can satisfy the damages element of a breach of contract claim." *Solara*, 2020 WL 2214152, at *5.

For these reasons, May's breach of contract claim in Count III will proceed.

IV. Conclusion

For the reasons explained above, this Court grants in part and denies in part Defendants' motions to dismiss [2]; [4].

As a result of the Court's rulings, the following claims are hereby dismissed from the consolidated amended complaint: the LDSBNL claim in Count XI; the implied contract claim in Count II as to all Plaintiffs but Parsons and Yeremian; the unjust enrichment claim in Count III; Myers' CCPA claim in Count IV; the CCRA claim in Count VI only as to Yeremian and Villalobos; the CMIA claim in Count VII as to all Plaintiffs; the UCL claims in Counts VIII and IX; the MPIPA claim in Count XIII; the Colorado statutory claims in Counts XVI and XVII; and the invasion of privacy claim in Count XVIII. The Court also notes that Plaintiffs have voluntarily dismissed their CLRA claim in Count V. All other claims remain pending in the consolidated amended complaint. Plaintiffs must file their amended complaint to cure the CCPA claim (Count IV) by October 14, 2022. Defendants are directed to answer by November 4, 2022.

As for May's complaint, this Court dismisses her UCL claim in Count II; May's other claims for violations of the CCPA and breach of express contract may proceed.

Defendants are directed to answer May's complaint by October 28, 2022.

All parties are directed to meet and confer and file a joint status report and proposed scheduling order by October 19, 2022. The parties shall propose discovery deadlines and explain why Ms. May has not been made a party to the consolidated complaint.

Dated: September 28, 2022

Entered:

Mary M. Rowland
United States District Judge