IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Southern Division

IN RE: MARRIOTT INTERNTIONAL, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	*	**MDL No. 19-md-2879**
CONSUMER ACTIONS	*	

* * * * * * * * * * * * * *

MEMORANDUM OPINION

This case involves the consolidated complaint filed by consumers against Marriott and related entities following one of the largest data breaches in history.[1] It is part of the Multidistrict Litigation ("MDL") pending before me concerning the data breach. The Plaintiffs and Marriott have selected ten "bellwether" claims to test the sufficiency of the pleadings.[2] Plaintiffs argue that Marriott is liable under theories of tort, contract, and statutory duties in various states. Defendants moved to dismiss, arguing that Plaintiffs lack standing and failed to state a claim. Def. Mot., ECF Nos. 450, 451.[3] For the reasons discussed below, Defendants' motion to dismiss Plaintiffs' claim for negligence under Illinois law is granted. Defendants motion to dismiss the remaining tort, contract, and statutory claims is denied.

---

[1] Second Amended Consolidated Complaint ("Compl."), ECF Nos. 413 (sealed), 537 (redacted). The Second Amended Consolidated Complaint is a superseding complaint as to all other complaints in this MDL filed on behalf of consumers. Compl. ¶ 6. Plaintiffs named as defendants Marriott International, Inc., Starwood Hotels & Resorts Worldwide, LLC, and Accenture LLP. Compl. ¶¶ 12–14. Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC will be referred to as "Defendants" or "Marriott" collectively, unless otherwise indicated. The claims against Accenture LLP are addressed in other briefings.

[2] *See* ECF No. 368 (selection of bellwether claims). Each party selected five claims, consisting of a cause of action and a jurisdiction from the Second Amended Consolidated Complaint, brought by the named plaintiffs from the relevant jurisdiction. *Id.* Unless otherwise indicated, "Plaintiffs" or "Bellwether Plaintiffs" refers to the plaintiffs selected for the purposes of this briefing.

[3] The motion has been fully briefed. *See* ECF Nos. 450, 473, 486 (redacted); ECF Nos. 451, 487, 494 (sealed). A hearing is not necessary. *See* Loc. R. 105.6 (D. Md. 2018).

Factual Background

On November 30, 2018, Marriott announced that it was the target of one of the largest data breaches in history. Compl. ¶ 1. The breach took place in its Starwood guest reservation database. Compl. ¶¶ 1, 172–93. Marriott International acquired Starwood Hotels & Resorts in September 2016. Compl. ¶ 98. This acquisition made Marriott the largest hotel chain in the world – accounting for 1 in 15 hotel rooms worldwide – with Marriott, Courtyard, Ritz-Carlton, Sheraton, Westin, W Hotels, and St. Regis properties under its umbrella. Compl. ¶ 98. When guests make a reservation to stay at a Marriott property, they must provide personal information including name, address, email address, phone number, and payment card information. Compl. ¶ 99. In some instances, Marriott also collects passport information, room preferences, travel destinations, and other personal information. Compl. ¶ 99. Both Marriott and Starwood had privacy statements, dated May 18, 2018 and October 5, 2014 respectively, concerning their collection and use of this personal information and touting their ability to protect the security of this sensitive information. Compl. ¶¶ 100–03, 113.

Investigations into the data breach indicated that for over four years, from July 2014 to September 2018, hackers had access to Starwood's guest information database. Compl. ¶ 2. In other words, the data breach was ongoing before and after Marriott's acquisition of Starwood. Plaintiffs allege that Marriott failed to conduct appropriate due diligence of Starwood's cybersecurity risks before and after the merger, despite the fact that Starwood disclosed a data breach affecting more than 50 locations days before Marriott's announcement of the merger, and after knowing that it and other hotel chains were the targets of security threats in the months and years preceding the data breach. Compl. ¶¶ 120; 139–65. Plaintiffs allege that several

cybersecurity assessments that were conducted revealed deficiencies in Starwood's system. Compl. ¶¶ 124–33.

During the course of the four-year data breach, the hackers allegedly stole names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, payment card expiration dates, and tools needed to decrypt cardholder data. Compl. ¶ 2. Further, several files that the hackers exfiltrated were deleted, so Marriott does not fully know how much data was stolen. Compl. ¶ 2. In total, Marriott allegedly disclosed that the breach impacted at least 383 million guest records, including nearly 24 million passport numbers and more than 9 million credit and debit cards. Compl. ¶ 3. Plaintiffs allege that Marriott discovered the breach on September 8, 2018 when Accenture (a consulting company providing cybersecurity assistance to defendants, and now a third-party defendant itself) reported an anomaly on Starwood's database, but that Marriott waited more than two months to notify guests. Compl. ¶¶ 178, 187, 194.

Plaintiffs are consumers who allegedly provided their personal information to Marriott to stay at a Marriott property or use Marriott's services before the data breach. *See* Compl. ¶¶ 25–28, 34–39, 42–43, 52–53, 55–56, 70–72, 77. Plaintiffs allege that Marriott is liable for the data breach under theories of tort, contract, and breach of statutory duties. The gravamen of these allegations is that Marriott failed to take reasonable steps to protect Plaintiffs' personal information against the foreseeable risk of a cyber attack and contrary to their express privacy statements and statutory duties.

Pending is Defendants' motion to dismiss the bellwether claims under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Defendants argue that most of the Plaintiffs lack standing and that all of the Plaintiffs failed to state claims upon which relief could be granted.

Standard of Review

Federal Rule of Civil Procedure 12(b)(6) provides for the dismissal of a complaint for "failure to state a claim upon which relief can be granted." This rule's purpose "is to test the sufficiency of a complaint and not to resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses." *Presley v. City of Charlottesville*, 464 F.3d 480, 483 (4th Cir. 2006). A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Specifically, plaintiffs must establish "facial plausibility" by pleading "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). But "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* Well-pleaded facts as alleged in the complaint are accepted as true. *See Aziz v. Alcolac*, 658 F.3d 388, 390 (4th Cir. 2011). And, factual allegations must be construed "in the light most favorable to [the] plaintiff." *Adcock v. Freightliner LLC*, 550 F.3d 369, 374 (4th Cir. 2008) (quoting *Battlefield Builders, Inc. v. Swango*, 743 F.2d 1060, 1062 (4th Cir. 1984)).

Where the allegations in a complaint sound in fraud, the plaintiff also must satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b) by "stat[ing] with particularity the circumstances constituting fraud." This requires that the plaintiff allege "the time, place, and contents of the false representations, as well as the identity of the person making the

misrepresentation and what he obtained thereby." *Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776, 784 (4th Cir. 1999) (internal quotation marks omitted).

Federal Rule of Civil Procedure 12(b)(1) governs motions to dismiss for lack of subject matter jurisdiction. *See Khoury v. Meserve*, 268 F. Supp. 2d 600, 606 (D. Md. 2003), *aff'd*, 85 F. App'x 960 (4th Cir. 2004). Under Rule 12(b)(1), the plaintiff bears the burden of proving, by a preponderance of evidence, the existence of subject matter jurisdiction. *See Demetres v. E. W. Constr., Inc.*, 776 F.3d 271, 272 (4th Cir. 2015); *see also Evans v. B.F. Perkins Co.*, 166 F.3d 642, 647 (4th Cir. 1999). A challenge to subject matter jurisdiction under Rule 12(b)(1) may proceed in two ways: either by a facial challenge, asserting that the allegations pleaded in the complaint are insufficient to establish subject matter jurisdiction, or a factual challenge, asserting "'that the jurisdictional allegations of the complaint [are] not true.'" *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009) (citing *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982)) (alteration in original); *see Buchanan v. Consol. Stores Corp.*, 125 F. Supp. 2d 730, 736 (D. Md. 2001). Here Defendants bring facial and factual challenges to Plaintiffs' Article III standing. Def. Mot. at 14.

In a facial challenge, "the facts alleged in the complaint are taken as true, and the motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Kerns*, 585 F.3d at 192. In a factual challenge "the district court is entitled to decide disputed issues of fact with respect to subject matter jurisdiction." *Id.* The court "may regard the pleadings as mere evidence on the issue and may consider evidence outside the pleadings without converting the proceeding to one for summary judgment." *Velasco v. Gov't of Indonesia*, 370 F.3d 392, 398 (4th Cir. 2004) (citing *Adams*, 697 F.2d at 1219 and *Evans*, 166 F.3d at 647).

Discussion

I. Standing

Marriott argues that most of the Bellwether Plaintiffs do not have standing, and therefore this Court lacks subject matter jurisdiction over their claims. Def. Mot. at 4.[4] Each of the elements of standing "must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Overbey v. Mayor of Baltimore*, 930 F.3d 215, 227 (4th Cir. 2019) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). "Thus, when a defendant challenges a plaintiff's standing, we analyze the challenge differently depending on the stage of litigation at which the challenge is brought and the substance of the defendant's arguments." *Id.* When, as here, "'standing is challenged on the pleadings, [the court will] accept as true all material allegations of the complaint and construe the complaint in favor of the complaining party.'" *Deal v. Mercer Cty. Bd. of Educ.*, 911 F.3d 183, 187 (4th Cir. 2018) (quoting *S. Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC*, 713 F.3d 175, 181–82 (4th Cir. 2013)). Therefore, to analyze standing, the Plaintiffs' allegations in their complaint will be accepted as true.

To establish standing, a plaintiff must have (1) "suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical," (2) "fairly traceable to the challenged action of the defendant," and (3) "likely . . . [to] be redressed by a favorable decision." *Bishop v. Bartlett*, 575 F.3d 419, 423 (4th Cir. 2009)); *see also Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992) (same). Defendants do not dispute that the alleged

[4] Plaintiffs challenge the standing of all bellwether plaintiffs, except plaintiffs Cullen, Golin, and O'Brien, who allege fraudulent misuse of their personal information. Def. Mot. at 17 n.12.

injuries could be redressed by a favorable decision. Rather, the challenge is whether particular Bellwether Plaintiffs have adequately alleged that they suffered injury-in-fact that is traceable to Defendants' conduct.

a. Plaintiffs Adequately Alleged Injury-In-Fact

Marriott argues that the fifteen Bellwether Plaintiffs that did not allege that their information was misused have not adequately alleged injury-in-fact. Def. Mot. at 4.[5] Plaintiffs argue that these plaintiffs have satisfied the injury-in-fact requirement by alleging (1) an imminent risk of injury of identity theft; (2) time and money expended to protect against identity theft; (3) loss of property value in their personal identifying information; and (4) loss of the benefit of their bargain with Marriott regarding data privacy. I agree and will discuss each in turn.

i. Imminent risk of injury of identity theft

Plaintiffs argue that they face an imminent threat of injury of identity theft based on their allegations that they provided personal information to Marriott, hackers targeted and stole this information, and this information has already been misused in some cases. *See, e.g.*, Compl. ¶¶ 2, 19, 36, 77; Opp. at 4–12. Defendants argue that this threat of injury is speculative and does not suffice to establish Article III standing. *See* Def. Mot. at 4–10. Two recent Fourth Circuit cases are instructive.

In *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), the Fourth Circuit considered two consolidated appeals – *Beck* and *Watson* – brought by veterans who received health care at the William Jennings Bryan Dorn Veterans Affairs Medical Center ("Dorn VAMC") in Columbia, South Carolina. In the *Beck* case, a laptop was stolen from Dorn VAMC that contained

[5] These plaintiffs are Guzikowski, Marks, Sempre, Maisto, Lawrence, Bittner, Long, Viggiano, Miller, Raab, Maldini, Ryans, Wallace, Gononian, and Fishon. Def. Mot. at 4 n.3.

unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors. *Id.* at 267. In the *Watson* case, Dorn VMAC discovered that four boxes of pathology reports were missing or stolen, which contained identifying information of over 2,000 patients including names, social security numbers, and medical diagnoses. *Id.* at 268. Plaintiffs in both cases alleged injury-in-fact based on the increased risk of identity theft. The courts disagreed. In the *Beck* case, the district court dismissed the claims for lack of standing on a summary judgment record. In the *Watson* case, the district court dismissed the claims for lack of standing based on the pleadings.

Relying on the Supreme Court's discussion of standing based on "threatened injuries" in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the Fourth Circuit affirmed the district court in both cases. The Fourth Circuit found that the harms alleged by the *Watson* and *Beck* plaintiffs were too speculative, because they required an "attenuated chain of possibilities." *Beck*, 848 F.3d at 275 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. at 410). Specifically, the court found that it was required to assume, "that the thief targeted the stolen items for the personal information they contained," and that "the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities." *Id.* But there was no indication that the laptop or the boxes of medical records were stolen for the purpose of identity theft in the first place or that any plaintiffs were victims of identity theft. Therefore, the court held this chain of possibilities was not sufficient to confer standing. *Id.*

In *Beck*, the Fourth Circuit also reviewed the decisions of its sister circuits. The Sixth, Seventh, and Ninth Circuits had found that an increased risk of future identity theft was sufficient to establish injury-in-fact. *See Beck*, 848 F.3d at 273 (citing *Galaria v. Nationwide Mut. Ins. Co.*,

663 Fed. Appx. 384, 387–89 (6th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 692, 694–95 (7th Cir. 2015); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010)). In contrast, the First and Third Circuits found that increased risk of identity theft did not constitute injury-in-fact. *Id.* at 273–74 (citing *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011)). The Fourth Circuit explained that in each of the cases where the plaintiffs had established injury-in-fact were "allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274. It summarized:

> In *Galaria*, *Remijas*, and *Pisciotta*, for example, the data thief intentionally targeted the personal information compromised in the data breaches. *Galaria*, 663 Fed. Appx. at 386 ("[H]ackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others."); *Remijas*, 794 F.3d at 694 ("Why else would hackers break into a store's database and steal consumers' private information?"); *Pisciotta*, 499 F.3d at 632 ("scope and manner" of intrusion into banking website's hosting facility was "sophisticated, intentional and malicious"). And, in *Remijas* and *Krottner*, at least one named plaintiff alleged misuse or access of that personal information by the thief. *Remijas*, 794 F.3d at 690 (9,200 of the 350,000 credit cards potentially exposed to malware "were known to have been used fraudulently"); *Krottner*, 628 F.3d at 1141 (named plaintiff alleged that, two months after theft of laptop containing his social security number, someone attempted to open a new account using his social security number).

Id. But in the case before it, neither the *Beck* nor *Watson* plaintiffs made claims regarding the targeting of their personal information for the purpose of identity theft or actual misuse of their information. Therefore, the alleged harm of identity theft was too speculative to establish injury-in-fact. *Id.* And because the threat of identity theft was too speculative, the cost of mitigative measures including the cost of credit monitoring services and the plaintiffs' time spent monitoring their financial and credit information was also insufficient to establish injury-in-fact. *Id.* at 276–77.

In *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018) the Fourth Circuit again considered whether the threat of identity theft was sufficient to establish injury-in-fact. In that case, the plaintiffs were three optometrists representing a putative class of victims whose personal information was allegedly stolen in a breach of a database maintained by the defendant, the National Board of Examiners in Optometry, Inc. ("NBEO"). *Id.* at 616. The NBEO had not publicly acknowledged whether it had suffered a data breach. *Id.* at 617. But by connecting the dots between them, the plaintiffs alleged that the NBEO's database had been breached and that as a result they suffered injuries including unauthorized credit cards opened in their names, an increased risk of identity theft, and the cost of time and money spent to mitigate further damages. *Id.* at 617–18. Applying *Beck*, the district court dismissed the claims, concluding that the plaintiffs' alleged harms were speculative and insufficient to establish injury-in-fact. *Id.* at 619.

But the Fourth Circuit reversed, distinguishing the case from *Beck*. The Fourth Circuit explained that in *Beck*, it "emphasized that a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Id.* at 621 (citing *Beck*, 848 F.3d at 274–75.) Whereas "[i]n *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes [containing personal information] had been stolen, but the information contained therein had not been misused[, the *Hutton* plaintiffs] allege[d] they have already suffered actual harm in the form of identity theft and credit card fraud." *Id.* at 621–22. Therefore, plaintiffs had been "concretely injured" by the data breach. *Id.* at 622.

Further, the Fourth Circuit held that "[a]t a minimum" these allegations were sufficient to establish standing based on "an imminent threat of injury." *Id.* at 622. The court explained that while in *Beck* "there was no evidence that the thief even stole the laptop with the intent to steal

private information . . . the [*Hutton*] Plaintiffs allege that their data has been stolen, accessed, and used in a fraudulent manner." *Id.* Finally, the Fourth Circuit held that given the non-speculative nature of these alleged injuries, the plaintiffs' out-of-pocket costs and time spent to mitigate the harms also constituted injury-in-fact. *Id.*

Thus in *Beck*, there was no injury-in-fact when there were not allegations that the personal information was targeted or misused, whereas in *Hutton*, injury-in-fact was established based on allegations of actual identity theft, the imminent threat of identity theft, and costs spent to mitigate identity theft given the allegations that the personal information was targeted and misused.

Here the complaint contains much more extensive allegations concerning the targeting of personal information for misuse than in *Beck* or *Hutton*, and, similar to *Hutton*, contains allegations of actual misuse by some of the plaintiffs. Unlike in *Beck* where there were no allegations of targeting, and in *Hutton* where the NBEO did not even acknowledge that a data breach occurred, here Marriott disclosed that it was the target of one of the largest sustained cyberattacks in history that compromised the personal information of up to 500 million hotel guests. *See* Compl. ¶¶ 1–3. And like the plaintiffs in *Hutton*, Bellwether Plaintiffs Hevener, Ropp, Cullen, Golin, and O'Brien allege actual misuse of their personal information. *See* Compl. ¶ 36 ("Subsequent to the Data Breach, Plaintiff Hevener suffered identity theft and fraud in the form of unauthorized credit cards applied for in her name"); ¶ 42 ("As a result of the Data Breach, Plaintiff Golin experienced unauthorized charges on [his] payment card"); *id.* ¶ 70 ("As a result of the Data Breach, Plaintiff Cullen experienced unauthorized charges on [his SPG] payment card, as well as unauthorized purchases made from his personal checking account"); *id.* ¶ 72 ("As a result of the Data Breach, Plaintiff O'Brien subsequently experienced unauthorized charges on [her] payment card"); *id.* ¶ 77 ("As a result of the Data Breach, Plaintiff Ropp suffered identity theft and fraud in the form

multiple unauthorized accounts for credit cards, consolidated loans, consumer accounts, and other lines of credit opened using his Personal Information"). These allegations bring the actual and threatened harm out the realm of speculation and into the realm of sufficiently imminent and particularized harm to satisfy the injury-in-fact requirement for Article III standing for all Bellwether Plaintiffs.

Defendants argue that the Bellwether Plaintiffs that did not themselves allege actual misuse have failed to establish injury-in-fact. While these Plaintiffs have not pled injury-in-fact based on identity theft that has already occurred, they have adequately pled imminent threat of identity theft. The question here is whether there are "allegations that suffice[] to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Beck*, 848 F.3d at 274. The allegations about the targeting of personal information in the cyberattack and the allegations of identity theft by other plaintiffs whose personal information was stolen makes the threatened injury sufficiently imminent. In other words, in these circumstances the remaining Bellwether Plaintiffs do not have to wait until they, too, suffer identity theft to bring their claims to this court.

Therefore, Bellwether Plaintiffs Hevener and Ropp have established injury-in-fact based on allegations of actual and threatened harm[6] and the remaining Bellwether Plaintiffs established injury-in-fact based on the non-speculative imminent threat of identity theft.

ii. Time and money spent to mitigate harms from the data breach

Plaintiffs allege that they spent time and money to mitigate harms from the data breach and argue that this is also establishes injury-in-fact. *See, e.g.*, Compl. ¶ 270(e)–(g), (k). Defendants argue that Plaintiffs cannot manufacture standing by choosing to make expenditures based on

[6] Defendants do not challenge the standing of plaintiffs Cullen, Golin, and O'Brien. *See* Def. Mot. at 17 n.12.

hypothetical future harm. As described above, in *Beck* the Fourth Circuit found that the cost of mitigative measures to protect against identity theft did not constitute injury-in-fact when the threat of identity theft was too speculative to constitute injury-in-fact. *Beck*, 848 F.3d at 276–77 ("Mitigation expenses do not qualify as actual injuries where the harm is not imminent.") (quoting *Remijas*, 794 F.3d at 694). In contrast, in *Hutton* the Fourth Circuit found that the time and cost of mitigative measures did constitute injury-in-fact where the threatened harm was sufficiently non-speculative to constitute injury-in-fact. *Hutton*, 892 F.3d at 622 ("Because the injuries alleged by the Plaintiffs are not speculative, the costs of mitigating measures to safeguard against future identity theft support the other allegations and together readily show sufficient injury-in-fact to satisfy the first element of the standing to sue analysis."). In other words, the two theories of injury-in-fact stand or fall together. Here because the alleged actual and threatened harm to the Bellwether Plaintiffs is sufficiently non-speculative to establish injury-in-fact, the Bellwether Plaintiffs have also established injury-in-fact based on the alleged time and money spent to mitigate that harm.

iii. Loss of value of property in their personal identifying information

Plaintiffs allege that they provided their personal identifying information ("PII") to Marriott and that as a result of the cyberattack they lost the value of that information. *See, e.g.*, Compl. ¶ 270(b). Defendants argue that this type of harm is not cognizable as a matter of law. Def. Mot. at 16.

The Fourth Circuit has not decided whether the loss of property value in personal identifying information constitutes a cognizable injury in data breach cases. But the growing trend across courts that have considered this issue is to recognize the lost property value of this information. *See In re Experian Data Breach Litig.*, No. SACV151592AGDFMX, 2016 WL

7973595, at *5 (C.D. Cal. Dec. 29, 2016) ("[A] growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory.") (quoting *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *43 (N.D. Cal. May 27, 2016)); *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014); *In re Yahoo!*, No. 16-MD-02752-LHK, 2017 WL 3727318, at 13 (N.D. Cal. Aug. 30, 2017). For example, in *In re Yahoo! Customer Data Sec. Breach Litigation* regarding a data breach of Yahoo! user accounts, Judge Koh explained that "Plaintiffs' allegations that their PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury arising from the Data Breaches." *In re Yahoo!*, 2017 WL 3727318, at *14.

Two courts in this district have taken a contrary view. In *Chambliss v. Carefirst, Inc*, the court found that plaintiffs did not establish injury-in-fact based on the decreased value of their personal information. 189 F. Supp. 3d 564, 572 (D. Md. 2016). That case involved a data breach of CareFirst, a health insurance provider, that compromised the personal information of 1.1 million individuals including "the names, birth dates, email addresses, and subscriber identification numbers of the affected individuals." *Id.* at 567. The court held that it "need not decide whether such personal information has a monetary value, as Plaintiffs have not alleged that they have attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information." *Id.* at 572. Similarly, in *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524, 533–34 (D. Md. 2016), the court rejected plaintiffs' allegations that they suffered loss of value in their personal identifying information. That case involved a data breach of the Children's Hospital in Washington, DC that compromised patient information including "names, addresses, dates of birth, Social Security numbers, and telephone numbers, as

well as private health care information." *Id.* 527. The court held that the alleged loss of value of personal information did not establish injury-in-fact because the plaintiff did not "explain how the hackers' possession of that information has diminished its value, nor does she assert that she would ever actually sell her own personal information." *Id.* at 533.

Here plaintiffs have adequately pled that the personal identifying information collected by Marriott has value. Plaintiffs allege that Marriott recognizes the value of this information and collects it to better target customers and increase its profits. Compl. ¶ 104. Marriott also pays a customer analytics company to analyze personal information for this purpose. *Id.* And Plaintiffs allege that this information is "highly-coveted and valuable on underground or black markets." Compl. ¶ 264.

The Complaint contains further allegations recognizing the value of personal information. For example, Commissioner Elizabeth Denham of the European Union, Information Commissioner's Office, which is investigating the Marriott data breach, stated, "Personal data has a real value so organizations have a legal duty to ensure its security, just like they would do with any other asset." Compl. ¶ 104. Similarly, the Court takes judicial notice of a recent statement by U.S. Attorney General William Barr announcing the indictment of four Chinese officials for the Equifax data breach, linking the attack to the Marriott data breach and recognizing the value of the personal information taken:

> For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, *the intrusion into Marriott hotels*, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax. *This data has economic value*, and these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages.

Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, February 10, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (emphasis added).

Neither should the Court ignore what common sense compels it to acknowledge – the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services. To take a few examples, many business offer goods and services such as wifi access, special access to products, or discounts in exchange for a customer's personal information. Consumer choose whether to exchange their personal information for these goods and services every day. And here, plaintiffs allege that they gave Marriott their personal information as part of their exchange to stay at Marriott hotels. Further, the value of personal identifying information is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their personal identifying information. Here Plaintiffs allege that they suffered lower credit scores as a result of the data breach and that fraudulent accounts and tax returns were filed in their names. *See, e.g.*, Compl. ¶¶ 36, 77, 104. Similarly, the businesses that request (or require) consumers to share their personal identifying information as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

For these reasons, I depart from the reasoning of *Chambliss* and *Khan* and am more persuaded by the growing number of courts that have recognized the loss of this property value in data breach cases. In *Chambliss* and *Khan*, the courts rejected alleged injuries based on the diminished value of personal information because the complaints did not allege that the plaintiffs

attempted to sell it themselves or that they were forced to accept a decreased price for their information. But the value of consumer personal information is not derived solely (or even realistically) by its worth in some imagined market place where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check. Therefore, the Bellwether Plaintiffs have established injury-in-fact based on the loss of value of their personal information.

iv. Loss of benefit of their bargain regarding data security

Plaintiffs also allege injury-in-fact based on "overpayment" and failure to receive the benefit of their bargain regarding data privacy. Specifically, plaintiffs allege that they "place significant value in data security," that "[t]he cost of purchasing a hotel room includes tangible and intangible components, including things such as the overall cost of the property and employee costs, as well the cost of providing conveniences like soaps and shampoos," that "[o]ne component of the cost of a hotel room is the explicit and implicit promises Marriott made to protect its customers' Personal Information," and that "had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their data—they would not have stayed at a Marriott Property, purchased products or services at a Marriott Property, and/or would have paid less." Compl. ¶ 273–75. Defendants again argue that this theory of injury fails as a matter of law. Def. Mot. at 16. The Fourth Circuit has not addressed this issue, and both Plaintiffs and Defendants marshal cases to support their position. For the reasons discussed below, I am persuaded that Plaintiffs have adequately alleged injury-in-fact based on failure to receive the benefit of their bargain regarding data security.

Plaintiffs point to *Carlsen v. GameStop, Inc.*, 833 F.3d 903 (8th Cir. 2016). In that case, the plaintiff paid for a subscription to Game Informer Magazine published by the defendant. *Id.* at 907. The terms of the magazine subscription included a privacy policy that stated subscribers' personal information would not be shared with third parties. *Id.* But the defendant allegedly shared this information with third parties nonetheless. Plaintiff alleged that he would not have paid as much as he did for the magazine subscription had he known that GameStop would violate the terms of the privacy policy. *Id.* at 908–09. The district court found that this overpayment theory was insufficient to establish injury because the plaintiff did not allege that he paid any specific amount for the privacy policy or that he bargained for additional data privacy. *Id.* at 909. The district court also rejected the argument that the plaintiff would not have purchased the magazine subscription had he known GameStop would have violated its privacy policy. *Id.* The Eighth Circuit reversed finding that the plaintiffs' allegations were sufficient to establish injury arising from a breach of contract:

> Here, Carlsen has provided sufficient facts alleging that he is party to a binding contract—the terms of service, which include the Game Informer privacy policy—with GameStop, and GameStop does not dispute this contractual relationship. Carlsen also has alleged that GameStop has violated that policy by "systematically disclos[ing] Game Informer's users' PII . . . to third party Facebook and/or allow[ing] Facebook to directly collect that information itself." This allegation of breach is both concrete and particularized, as the breach allegedly already has occurred, and any consequences of the breach have occurred specifically to Carlsen as a result of the actions of GameStop's alleged systematic disclosure via the Facebook SDK.

Id. The Eighth Circuit also found that these same allegations were sufficient to establish injury based on an overpayment theory. *See id.* ("Carlsen alleged that he has suffered damages as a result of GameStop's breach in the form of devaluation of his Game Informer subscription in an amount equal to the difference between the value of the subscription that he paid for and the value of the subscription that he received, *i.e.*, a subscription with compromised privacy protection.

Accordingly, Carlsen has alleged an 'actual' injury.") Thus, the allegations plausibly established injury from breach of contract and alternatively breach leading to a devaluation of the goods purchased.

Similarly, the court in *In re Yahoo! Inc. Customer Data Sec. Breach Litigation* found that the plaintiff adequately alleged benefit-of-the-bargain losses. 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018). In that case, the plaintiff alleged that he paid for Yahoo!'s premium email service, that Yahoo! represented that their email services were secure, and that that he would not have provided his personal information to Yahoo! or signed up for the email services if he knew they were not as secure as Yahoo! represented. *Id.* Thus, plaintiff alleged that the services he paid for were worth nothing or worth less than he paid for them. *Id.* The court held that this established benefit-of-the-bargain injury. *Id. See also In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) (finding plaintiffs adequately pled benefit-of-the-bargain losses); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F.Supp.3d 1197, 1224 (N.D.Cal.2014) (finding plaintiffs adequately pled injury where they alleged "they personally spent more on Adobe products than they would had they known Adobe was not providing the reasonable security Adobe represented it was providing.")

Defendants argue that Plaintiffs' allegations fail as a matter of law to establish injury-in-fact, again pointing to *Chambliss*. There the court found that the plaintiffs made no allegations that "the data breach diminished the value of the health insurance they purchased from CareFirst" or "indicating that the prices they paid for health insurance included a sum to be used for data security, and that both parties understood that the sum would be used for that purpose." *Chambliss v. Carefirst, Inc*, 189 F. Supp. 3d 564, 572 (D. Md. 2016). Further, the court stated that the plaintiffs could not quantify their alleged losses. *Id.*

Defendants also cite cases for the proposition that it is improper to "chop up a contract" for data security. In *Irwin v. Jimmy John's Franchise, LLC*, plaintiffs brought a putative class action for alleged injuries arising from a data breach at Jimmy John's restaurants. 175 F. Supp. 3d 1064 (C.D. Ill. 2016). One of the claims brought by the plaintiffs was for unjust enrichment, for which the plaintiffs alleged Jimmy John's was enriched, and the plaintiffs were impoverished, because Jimmy John's accepted plaintiff's credit and debit card payments without providing security and protection. The court rejected the unjust enrichment claim, finding that data security was not paid for separately:

> Irwin paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase, as is the ability to sit at a table to eat her food, or to use Jimmy John's restroom. Jimmy John's would not be enriched by customers who paid full price for their purchases but found all tables occupied, or a restroom temporarily out of order. The court is further persuaded by the fact that merchants are assessed a fee for each debit and credit card transaction, and merchants sometimes offer a discount for cash payment. *See, e.g.*, Consumer Reports, *Don't be Tricked by Gas Station Cash Discounts*, available at http://www.consumerreports.org/cro/news/2013/08/gas-station-cash-discounts/index.htm. Irwin does not allege that she paid more than cash customers did for the same food items, so it cannot be said that Jimmy John's was unjustly enriched by her purchases.

Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064 at 1071–72 (C.D. Ill. 2016).[7] But the court did find that find that plaintiff plausibly alleged an implied contract for data security based on her use of a debit or credit card for payment. *See Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1070–71 (C.D. Ill. 2016) ("When the customer uses a credit card for a

[7] The court did not appear to consider the benefit that Jimmy John's derived by accepting debit and credit cards. Instead, it seems the court was persuaded that because Jimmy John's pays credit card fees, it does not benefit from accepting debit and credit cards as a form of payment. But as the Supreme Court recently explained, while credit card companies like American Express charge merchants fees, accepting payment cards "benefit[s] merchants by encouraging cardholders to spend more money." *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2283 (2018). Therefore, the *Irwin* court did not appear to consider the full scope of benefits in its analysis.

commercial transaction, he intends to provide the data to the merchant, and not to an unauthorized third party. There is an implicit agreement to safeguard the customer's information to effectuate the contract. Irwin has alleged the existence of an implied contract obligating Jimmy John's to take reasonable measures to protect Irwin's information and to timely notify her of a security breach.") (internal citation omitted).

Defendants also cite *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016). In that case the court expressed skepticism but did not decide whether the plaintiffs established injury-in-fact based on allegations that the costs of the plaintiffs' meals were an injury because they would not have dined at P.F. Chang's had they known of its poor data security. *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d at 968. The court said that, "such arguments have been adopted by courts only where the product itself was defective or dangerous and consumers claim they would not have bought it (or paid a premium for it) had they known of the defect." *Id.* The *P.F. Chang's* plaintiffs did not allege this. *Id.*

Likewise, in *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014), the court rejected an overpayment theory of injury in a data breach case involving theft of personal information and medical records of 4.7 million members of the U.S. military and their families. The court stated:

> [A]s to the value of their insurance premiums, Plaintiffs do not plausibly allege any actual loss. They allege that they were paying for "health and dental insurance"—and they do not claim that they were denied coverage or services in any way whatsoever. *See id.* To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing. They do not maintain, moreover, that the money they paid could have or would have bought a better policy with a more bullet-proof information-security regime. Put another way, Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid. Nothing in the Complaint makes a plausible case that Plaintiffs were cheated out of their premiums. As a result, no injury lies.

In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 30 (D.D.C. 2014).

Here the pleadings are similar to those in *Carlson*, *In re Yahoo!*, and *In re Anthem*. Like the plaintiffs in those cases, Plaintiffs here allege that there was an explicit or implicit contract for data security based on Marriott and Starwood's privacy statements,[8] that they placed a significant value in data security, and that had they known the truth about Marriott's data security practices they would have paid less or not stayed at Marriott. Compl. ¶ 273–75.

In this regard the pleadings differ from those in *Chambliss*, *Irwin*, *Lewert*, and *In re SAIC*. Whereas in *Chambliss* the court noted that the plaintiffs failed to make allegations that the data breach diminished the value of their health insurance, here plaintiffs specifically allege that they value data security and Marriott's misrepresentations in this regard diminished the value of their purchases. And to the extent these courts found that plaintiffs did not pay separately for data security in those transactions, I find it unnecessary at this stage to parse out what portion of the bargain between Plaintiffs and Marriott can be attributed to data security. As the courts in *Carlson*, *In re Yahoo!*, and *In re Anthem* found, it is enough to allege that there was an explicit or implicit contract for data security, that plaintiffs placed value on that data security, and that Defendants failed to meet their representations about data security. Valuation of these alleged damages may be done after discovery. Therefore, plaintiffs have adequately alleged injury based on their benefit-of-the-bargain and overpayment theories.

[8] For further discussion of the express and implied contract claims, see Section III below.

b. Plaintiffs' Injuries Are Fairly Traceable to Defendants' Conduct

Defendants argue that two of the Bellwether Plaintiffs that alleged actual misuse – Hevener and Ropp – lack standing because their alleged injuries are not fairly traceable to Defendants' conduct. Def. Mot. at 17. Plaintiff Hevener alleges that as a result of the data breach, unauthorized credit cards were applied for in her name. Compl. ¶ 36. And Plaintiff Ropp alleges that because of the data breach multiple unauthorized accounts for credit cards, consolidated loans, consumer accounts, and other lines of credit were opened using his personal information. Compl. ¶ 77. Defendants also argue that the alleged injuries of a third bellwether plaintiff, Cullen, stemming "unauthorized purchases made from his personal checking account" are not traceable to the Marriot data breach, but do not challenge Cullen's standing based on his allegations of payment card misuse. Def. Mot. at 17 n.2.

Defendants argue that these injuries are not fairly traceable to Defendants because these injuries purportedly require social security numbers or banking information which no plaintiff alleges to have given to Marriott. Def. Mot. at 17. To support this proposition, Defendants cite to several cases that discuss the use of social security numbers to open accounts. *See Hutton v. Nat'l Bd. Of Examiners in Optometry, Inc.*, 892 F.3d 613, 623 (4th Cir. 2018); *In re SuperValu, Inc.*, 925 F.3d 955, 960 (8th Cir. 2019); *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016); *Antman v. Uber Techs., Inc.*, 2018 WL 2151231, at *6, 10-11 (N.D. Cal. May 10, 2018). But in only one of these cases, *Antman*, did a court dismiss a claim in which a plaintiff alleged fraudulent accounts were applied for or opened in his or her name due to lack of traceability.

In *Hutton*, the plaintiffs alleged that social security numbers were stored by the defendant, which supported their claim for standing. 892 F.3d at 623. The court did not find, or even consider,

that traceability is not established where social security numbers were not collected. The courts in *In re Supervalu, Inc.* and *Dugas* considered the scope of information allegedly stolen, including social security numbers, when assessing the risk of imminent threat of identity theft. For the reasons discussed above, the Plaintiffs here have met this threshold. Moreover, those courts found standing for the plaintiffs that did allege fraudulent card charges. *See In re SuperValu, Inc.*, 870 F.3d at 773; *Dugas*, 2016 WL 6523428, at *6. In *Antman*, the plaintiff alleged that only drivers' licenses and names were stolen in a data breach, and at oral argument plaintiff's counsel conceded that a social security number was required for the fraudulent Capitol One credit card application in question. *Antman*, 2015 WL 6123054, at *8, *11. On that basis the court found injury stemming from the fraudulent Capitol One application was not fairly traceable to defendant's data breach. *Id.* at *11.

Other cases have found that stolen credit card information, even without social security numbers, was enough to commit identity theft and fraud. *See, e.g.*, *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) ("Although there is no allegation in this case that the stolen information included social security numbers . . . the information taken in the data breach still gave hackers the means to commit fraud or identity theft . . . ."); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) ("We recognized in *Remijas* [794 F.3d at 692–93] that the information stolen from payment cards can be used to open new cards in the consumer's name."); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1034 (N.D. Cal. 2019) (finding personal information, not including social security numbers, "gave hackers the means to commit fraud or identity theft.")

Here plaintiffs Hevener, Ropp, and Cullen allege that they stayed at Marriott properties, that they gave their personal information to Marriott to do so, that Marriott was the target of one

of the largest data breaches in history – the scope of which is not yet fully known – and that as a result, fraudulent accounts were opened or applied for in their names. Plaintiffs have adequately alleged their injuries are traceable to Defendants' conduct. While Defendants may ultimately show, after the opportunity for discovery, that the alleged injuries are not caused by their data breach, it is premature to dismiss Plaintiffs' claims on grounds of traceability.

Thus, for the reasons stated above, all Bellwether Plaintiffs have standing. I now turn to the bellwether claims selected by the parties.

II. Negligence Claims

Bellwether Plaintiffs allege negligence claims under the laws of three states: Illinois, Florida, and Georgia. Defendants move to dismiss each claim. For the reasons discussed below, Defendants' motion to dismiss the Illinois negligence claim is granted. Defendants' motion to dismiss the Florida and Georgia claims is denied. I discuss the negligence claims of each state in turn.[9]

a. Illinois Negligence Claims

Illinois class representatives Golin and Raab bring claims for negligence under Illinois law. *See* Compl. ¶¶ 42–43; 296–304; ECF No. 368. Marriott argues that these claims must be dismissed because the "economic loss rule" precludes the Plaintiffs from recovering against it for damages that do not result from personal injuries or physical damage to tangible property, and because Illinois law does not impose a duty on retailers to safeguard personal information from cyberattacks. Def. Mot. at 18–19.

[9] Under *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938), for each of the tort, contract, and statutory claims discussed below, I must apply the jurisprudence of the relevant state's highest court or, if it has not spoken to the issue, predict how the state's highest court would rule. *See Private Mortg. Inv. Servs., Inc. v. Hotel & Club Assocs., Inc.*, 296 F.3d 308, 312 (4th Cir. 2002).

i. Economic Loss Rule

The economic loss rule bars recovery in tort for "economic losses," and instead requires personal injury or property damage to support a negligence claim. *See Moorman Mfg. Co. v. Nat'l Tank Co.*, 435 N.E.2d 443, 449 (Ill. 1982). As a threshold matter, the parties dispute whether all of Plaintiffs' alleged injuries are economic, such that they would be precluded by the rule. The parties appear to agree that some of the injuries, including unauthorized charges, money spent to mitigate harms of the breach, and benefit-of-the-bargain losses, are economic in nature. However, Plaintiffs argue that the alleged loss of value of their personal information, time spent mitigating harm from the data breach, and personal aggravation arising from the increased risk of identity theft are non-economic injuries that fall outside the scope of the economic loss rule. Opp. at 17.

To support their position, Plaintiffs cite *Morris v. Harvey Cycle & Camper, Inc.*, 911 N.E.2d 1049 (Ill. App. Ct. 2009). In that case, the plaintiff brought a claim under the Illinois Consumer Fraud Act following problems with the financing and purchase of a car and alleged "severe emotional distress, inconvenience and aggravation." *Id.* at 1052–53. The Illinois Consumer Fraud Act provides a remedy for purely economic injuries. *Id.* The Court of Appeals affirmed the Circuit Court's dismissal of the plaintiff's Consumer Fraud Act claim, finding that "she did not allege actual damages in the form of specific economic injuries" and that "[s]he alleged only emotional damages." *Id.* In other words, in the context of stating an Illinois Consumer Fraud Act claim, emotional distress, inconvenience, and aggravation were all deemed non-economic injuries. And Plaintiffs point to cases outside of Illinois to support their argument that the loss of value of personal information and loss of time are non-economic injuries that are outside the scope of the economic loss rule. *See Hameed-Bolden v. Forever 21 Retail, Inc.*, No. CV1803019SJOJPRX, 2018 WL 6802818, at *5 (C.D. Cal. Oct. 1, 2018) (noting that loss of value

in personal information "may represent 'property damages' as a legal matter," but ultimately finding that plaintiffs failed to establish that theft of their personal information damaged them in a non-economic manner); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019) (holding plaintiffs' alleged loss of time was not economic injury and therefore economic loss rule did not bar negligence claim under California law).

In response, Defendants cite *Fox v. Iowa Health System*, 399 F. Supp. 3d 780 (W.D. Wis. 2019). In that case, which involved a data breach of a health system, the court dismissed the plaintiffs' Illinois negligence claims under the economic loss doctrine. The plaintiffs argued that some of their injuries, including their lost time, loss in the value of their personal information, and damages caused by the violation of their privacy rights, were outside the scope of the economic loss rule. *Id.* at 795. The court disagreed, finding that "all of these are economic damages because they reflect a pecuniary loss rather than a personal injury or damage to property." *Id.* (citing *In re Illinois Bell Switching Station Litigation*, 641 N.E.2d 440, 444 (Ill. 1994) (finding damages incurred from a month-long loss of telephone services were economic damages)). Further, the court found that "claims for inconvenience or lost time fall squarely within the economic loss doctrine." *Id.* (citing *Followell v. Cent. Illinois Pub. Serv. Co.*, 663 N.E.2d 1122, 1124 (Ill. App. Ct. 1996) (finding that lost time and profits to repair water mains and meters due to mismarked gas lines were economic damages)).

Taken together, *Morris* suggests that that an Illinois Court would find that Plaintiffs' claims for aggravation are not economic injuries but *Fox* and *Followell* suggest that claims for lost time are economic injuries. And although the court in *Fox* cites *Illinois Bell* to support its conclusion that the loss of value of personal information is an economic injury, neither *Fox* nor *Illinois Bell* discusses this specific issue. Moreover, the Illinois Supreme Court has yet to address the economic

loss rule in the context of data breaches at all. An examination of the rule's development suggests that its historical roots in products liability are not a close fit with the injuries that arise in the context of data breaches like this one, which casts doubt on how it would be applied by the Illinois Supreme Court. Therefore, I must review the rule's development more fully.

The economic loss rule is of relatively recent vintage and was most prominently articulated by Chief Justice Traynor of the Supreme Court of California in *Seely v. White Motor Company*, 403 P. 2d 145 (Ca. 1965). The rule attempts to draw a line of demarcation between when it is appropriate for a plaintiff to recover in tort against a defendant, and when, in contrast, the recovery must be under contract or warranty law. The Illinois Supreme Court first adopted the economic loss rule in *Moorman Mfg. Co. v. National Tank Co.*, 435 N.E. 2d 443 (Ill. 1982). In *Moorman*, the plaintiff, a food processor, sued the manufacturer of a steel bolted grain storage tank under astrict liability theory (as well as misrepresentation and breach of warranty) when a crack developed in one of the steel rings of the tank, asserting that its negligent design made it unreasonably dangerous. It sought damages for the cost of repairs of the tank, as well as for the loss of its use in its business. *Id.* at 445. The Illinois Supreme Court emphasized that an action for strict liability is intended to allow recovery for the unreasonably dangerous nature of a product, which may result in the buyer's personal injury or physical injury to his property. *Id.* at 446–47. It contrasted this theory of recovery with the law of sales, which was "carefully articulated to govern the economic relations between suppliers and consumers of goods." *Id.* at 447 (citing numerous sections of Title 2 of the Illinois Uniform Commercial Code ("UCC")). The court expressed concern that "adopting strict liability in tort for economic loss would effectively eviscerate section 2-316 of the UCC" (which addresses the degree to which parties to a sales

contract may exclude warranties, and prohibits a manufacturer from disclaiming its responsibility for defective products). *Id.* at 447. It summed up its reasoning as follows:

> We do hold, however, that when a product is sold in a defective condition that is unreasonably dangerous to the user or consumer or to his property, strict liability in tort is applicable to physical injury to plaintiff's property, as well as to personal injury. . . . This comports with the notion that the essence of a product liability tort case is not that the plaintiff failed to receive the quality of the product he expected, but that the plaintiff has been exposed, through a hazardous product, to an unreasonable risk of injury to his person or property. On the other hand, contract law, which protects expectation interests, provides the proper standard when a qualitative defect is involved, i.e. when a product is unfit for its intended use.

Id. at 448–49.

The court then proceeded to explain the contours of "economic loss" that falls within the scope of the rule:

> "Economic loss" has been defined as "damages for inadequate value, costs of repair and replacement of the defective product, or consequent loss of profits – without any claim of personal injury or damage to other property" as well as "the diminution in the value of the product because it is inferior in quality and does not work for the general purposes for which it was manufactured and sold." These definitions are consistent with the policy of warranty law to protect expectations of suitability and quality.

Id. at 449 (internal citations omitted). The court also held that economic loss includes "all indirect loss, such as loss of profits resulting from inability to make use of the defective product." *Id.* at 449. And, it summed up its views of where the line of demarcation between tort and contract law lies as follows:

> [T]he line between tort and contract must be drawn by analyzing interrelated factors such as the nature of the defect, the type of risk, and the manner in which the injury arose. These factors bear directly on whether the safety-insurance policy of tort law or the expectation-bargain protection policy of warranty law is most applicable to a particular claim. . . . Our conclusion that qualitative defects are best handled by contract, rather than tort, law applies whether the tort theory involved is strict liability or negligence. Tort theory is appropriately suited for personal injury or property damage from a sudden or dangerous occurrence of the nature described above. The remedy for economic loss, loss relating to a purchaser's disappointed

> expectations due to deterioration, internal breakdown or nonaccidental cause, on the other hand, lies in contract.

Id. at 450–51 (internal quotation marks and citation omitted). Thus, while the court grounded its analysis of the economic loss rule in products liability law, it went on to extend it to ordinary negligence actions as well, again citing Chief Justice Traynor:

> (A consumer) can, however, be fairly charged with the risk that the product will not match his economic expectations unless the manufacturer agrees that it will. *Even in actions for negligence, a manufacturer's liability is limited to damages for physical injuries and there is no recovery for economic loss alone.*

Id. at 451 (citing *Seely*, 403 P. 2d at 151) (emphasis added).

The court further explained why the economic loss rule applies to negligence claims as well as product liability claims as follows:

> The policy considerations against allowing recovery for solely economic loss in strict liability cases apply to negligence actions as well. When the defect is of a qualitative nature and the harm relates to the consumer's expectation that a product is of a particular quality so that it is fit for ordinary use, contract, rather than tort, law provides the appropriate set of rules for recovery. Moreover, as was true with strict liability, if a manufacturer were held liable in negligence for the commercial loss suffered by a particular purchaser, it would be liable for business losses of other purchasers, caused by the failure of its product to meet the specific needs of their businesses, even though the needs were communicated only to the dealer. Thus, a manufacturer could be held liable for damages of unknown and unlimited scope, even though the product is not unreasonably dangerous and even though there is no damage to person and property.

Id. at 451–52 (internal citations omitted). Finally, the Illinois Supreme Court recognized two narrow exceptions to the economic loss rule. "This court has held that economic loss is recoverable where one intentionally makes false representations, and where one who is in the business of supplying information for the guidance of others in their business transactions makes negligent representations." *Id.* at 452 (internal citations omitted).

Shortly after *Moorman* was decided, the Illinois Supreme Court again addressed the economic loss rule in *Redarowicz v. Ohlendorf*, 441 N.E. 2d 324 (Ill. 1982). There, a homeowner

purchased a house from the original owner, discovered serious construction defects in the structure, and sued the builder asserting claims in negligence, contract, and warranty. The court declined to analyze whether the builder owed the plaintiff a duty in tort, instead holding that the damages sought by the plaintiff (repair or replacement of a defective chimney, wall and patio) were economic losses, and the negligence claim was barred by the *Moorman* doctrine. The court explained that "[t]o recover in negligence there must be a showing of harm above and beyond disappointed expectations. A buyer's desire to enjoy the benefit of his bargain is not an interest that tort law traditionally protects." *Id.* at 327. And the court quoted with approval a decision from the Supreme Court of Missouri, *Crowder v. Vandendeale*, 564 S.W. 2d 879 (Mo. 1978), which held:

> A duty to use ordinary care and skill is not imposed in the abstract. It results from a conclusion that an interest entitled to protection will be damaged if such care is not exercised. Traditionally, interests which have been deemed entitled to protection in negligence have been related to *safety* or freedom from physical harm. Thus, where personal injury is threatened, a duty in negligence has been readily found. Property interests also have generally been found to merit protection from physical harm. However, where mere deterioration or loss of bargain is claimed, the concern is with a failure to meet some standard of quality. This standard of *quality* must be defined by reference to that which the parties have agreed upon.

Id. at 882 (emphasis in original).

In *Anderson Elec. v. Ledbetter Erection Corp*., 503 N.E. 2d 246 (Ill. 1986), the Illinois Supreme Court extended the *Moorman* doctrine to a claim where the plaintiff asserted negligent performance of services. In *Ledbetter*, the plaintiff was an electrical subcontractor that contracted to perform work for Ledbetter, a general contractor, on precipitator units manufactured by Walther. *Id.* at 247. Anderson's contract with Ledbetter required it to perform its work in accordance with Walther's precipitator unit erection manual, which required Walther to inspect the project in stages as it was being performed, to insure compliance with the manual, and immediate correction of any

noted defects before the next phase of work commenced. *Id.* But Anderson had no contractual relationship with Walther. *Id.* Apparently, Walther did not inspect until Anderson completed all its work, and found defects that required that much of the work be redone, at a cost to Anderson of $288,802.44, significantly reducing its profit on the subcontract. *Id.* Anderson sued Walther for negligent failure to inspect the construction in phases as required by its manual.

Citing *Moorman*, the Illinois Supreme Court affirmed the decision of the Illinois Court of Appeals upholding the trial court's dismissal of Anderson's claim under the economic loss rule, noting that without concomitant claims of personal injury or damage to property other than the product that was the subject of the underlying contract (the precipitator unit), tort law afforded no remedy. *Id.* at 247 (quoting *Moorman*). In reaching its conclusion, the Illinois Supreme Court cited with approval a decision from the United States Supreme Court, *East River Steamship Corp. v. Transamerica Delava, Inc.*, 476 U.S. 858 (1986), which also addressed the economic loss rule, again in a products liability claim. In that case, the U.S. Supreme Court discussed the distinction drawn between tort recovery (for physical injuries) and warranty recovery (for economic loss), observing:

> The distinction rests . . . on an understanding of the nature of the responsibility a manufacturer must undertake in distributing his products. When a product injures only itself the reasons for imposing a tort duty are weak and those for leaving the party to its contractual remedies are strong. The tort concern with safety is reduced when an injury is only to the product itself. When a person is injured, the 'cost of an injury and the loss of time or health may be an overwhelming misfortune', and one the person is not prepared to meet. In contrast, when a product injures itself, the commercial user stands to lose the value of the product, risks the displeasure of its customers who find that the product does not meet their needs, or, as in this case, experiences increased costs in performing a service. Losses like these can be insured."

Id. at 871 (internal citations and quotation marks omitted).

But in *Collins v. Reynard*, 607 N.E. 2d 1185 (Ill. 1992), the Illinois Supreme Court recognized that there can be circumstances in which an injured party may sue in both contract and tort, despite the absence of personal injury or physical damage to property. In *Collins*, the plaintiff sued her attorney for negligence in preparing documents for the sale of a business. The court explained its ruling this way:

> Today we rule that a complaint against a lawyer for professional malpractice may be couched in either contract or tort and that recovery may be brought in the alternative . . . . Our ruling is grounded on historical precedent rather than logic. If something has been handled in a certain way for a long period of time and if people are familiar with the practice and accustomed to its use, it is reasonable to continue with that practice until and unless good cause is shown to change the rule.

Id. at 1186.

In explaining why it overruled the decision by the Court of Appeals that *Moorman* precluded suing an attorney for malpractice in tort, the Illinois Supreme Court again ventured into a discussion of the underlying policies that distinguish contract claims from tort claims:

> Contract law applies to voluntary obligations freely entered into between parties. Damages recoverable under a breach of contract theory are based upon the mutual expectations of the parties. The basic principle for the measurement of contract damages is that the injured party is entitled to recover an amount that will put him in as good a position as he would have been had the contract been performed as agreed.
>
> Tort law, on the other hand, applies in situations where society recognizes *a duty to exist wholly apart from any contractual undertaking*. Tort obligations are general obligations that impose liability when a person *negligently, carelessly or purposely causes injury to others.* These obligations have been recognized by society to protect fellow citizens from unreasonable risks of harm. *Whether a duty will be recognized under tort law depends upon the foreseeability of the injury, the likelihood of the injury, the magnitude of the burden of guarding against the injury, and the consequences of placing that burden on the defendant.*
>
> Although the common law distinctions between contract and tort have been both modified and confused by different courts in different situations, differences between tort theories and contract theories still have validity. For all of that, a punch in the nose remains, for all practical purposes, a tort and not a breach of

> contract. *In the field of contract, however, some breaches have crossed the line and become cognizable in tort.*

Id. at 1186–87 (internal citations omitted; emphasis added). But having opened the door that *Moorman* created separating contract from tort, the Illinois Supreme Court was quick to insure that only a crack remained open, adding "the ruling we announce today is limited to the specific field of lawyer malpractice as an exception to the so-called *Moorman* doctrine and to the distinctions separating contract from tort." *Id*. at 1187. But it did not take long before that crack was widened.

In *Congregation of the Passion, Holy Cross Province v. Touche Ross & Co*., 636 N.E. 2d 503 (Ill. 1994), the Illinois Supreme Court again was thrust into a dispute centering around the scope of the *Moorman* doctrine. After a Catholic church suffered severe financial losses caused by the failure of their accountant properly to value certain assets held by the church to generate income enabling it to operate its monasteries, retreat houses and schools, it sued its accounting firm and obtained substantial trial verdicts under both its negligence and contract claims. Notwithstanding its proclamation in *Collins* that it was relaxing the *Moorman* doctrine only to accommodate tort claims against an attorney for malpractice (for reasons based not on logic, but rather historical tradition), the Illinois Supreme Court extended the *Collins* exception to suits against accountants as well. To reach this result, it distilled the progression of its cases interpreting the economic loss rule from its adoption in *Moorman* this way:

> The evolution of the economic loss doctrine shows that the doctrine is applicable to the service industry only where the duty of the party performing the service is defined by the contract that he executes with his client. Where a duty arises outside of the contract, the economic loss doctrine does not prohibit recovery in tort for the negligent breach of that duty.

Id. at 514. Importantly, the court held that the "duty to observe reasonable professional competence exists independently of any contract. The economic loss doctrine does not bar recovery in tort for the breach of a duty that exists independently of a contract." *Id.* at 515.

Although the Illinois Supreme Court has further addressed the scope of the *Moorman* doctrine in the years since the *Congregation of the Passion* decision, the parties have not cited, and my own research has not located, any appellate decision by either the Court of Appeals or Supreme Court of Illinois that evaluated the applicability of the economic loss rule for a negligence claim in a data security breach, such as the claim involved in the MDL pending before me. However, several federal courts have applied the rule in data breach cases, including the United States District Court for the Northern District of Illinois in *In re Michaels Stores Pin Pad Litigation*, 830 F. Supp. 2d 518 (N.D. Ill. 2011) ("*Michaels Pin Pad*"). In his thoughtful decision, Judge Charles P. Kocoras analyzed Illinois law as it applied to the viability of the putative class plaintiffs' negligence claims against Michaels Stores, an arts and crafts retailer with stores throughout Illinois and the United States, arising out of a data security breach that resulted in the loss of customer personal financial information. Judge Kocoras ultimately concluded that the *Moorman* doctrine prevented the plaintiffs from stating a claim for negligence against the retailer.

The underlying facts of the *Michaels Pin Pad* case are familiar to any consumer in the United States (and likely abroad). When customers checked out at the cash register of a Michaels store, they were required to "swipe" their bank card on a "pin pad" device if they wished to pay for their purchase by a credit or debit card, a process that might require them to input their Personal Information Number ("PIN"). When they did, the pin pad stored their PIN and bank card information (supposedly securely) to allow verification with the bank that issued the bank card. *Id.* at 521. But "skimmers," criminals who replace legitimate pin pads with ones modified to

enable them to steal the bank card information and PIN, had placed modified pin pads in a number of Michaels stores in Illinois. Once they obtained customer bank card and PIN, they either sold the information to others or used it to create a fake bank card in the name of the unsuspecting consumer victim. *Id.* at 521–22.

The plaintiffs in *Michaels Pin Pad* were class representatives of Michaels customers that claimed they had sustained a variety of damages as a result of Michaels' failure to prevent the theft of their personal financial information. Their claims included negligence and negligence per se tort claims. Michaels sought to dismiss the negligence (and other) claims, contending that the *Moorman* doctrine precluded the plaintiffs from bringing a negligence claim, and the plaintiffs did not dispute that they sought to recover only economic losses. *Id.* at 530.

Judge Kocoras began his analysis with a thorough discussion of the decisions of the Illinois Supreme Court analyzing the economic loss rule, beginning with *Moorman*. Ultimately, he rejected the Plaintiffs' argument that the economic loss rule was inapplicable because the duty to protect their financial information arose independently from any contractual obligation or warranty, concluding that the "independent duty" exception to the *Moorman* doctrine announced by the *Congregation of the Passion* case was inapplicable, because the "ultimate result of the transaction was the sale of the products to Plaintiffs, not the provision of intangible services." *Id.* at 530. And, citing to the decisions of courts in other jurisdictions that had dismissed data breach negligence claims on the basis of the economic loss rule, he dismissed the negligence claims. *Id.* at 531.[10] Following *Michaels Pin Pad,* several other federal courts have denied Illinois negligence

[10] *See In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) (citing I*n re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d at 498–99; *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175–77 (3d Cir. 2008); *Cumis Ins. Society, Inc. v. BJ's Wholesale Club, Inc.*, 918 N.E.2d 36, 46–47 (Mass. 2009).

claims based on the economic loss rule. *See Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 794–95 (W.D. Wis. 2019); *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 817 (7th Cir. 2018); *In re Target Corp.*, 66 F. Supp. 3d 1154, 1174 (D. Minn. 2014).

However, I have doubts about whether a sufficiently full consideration has been given to the policies that justified the adoption of the economic loss rule, their continued application to modern digital commercial transactions, and the true nature of the injuries suffered by victims of data security breaches.[11] The progression of cases decided by the Illinois Supreme Court since its adoption of the economic loss rule demonstrates that it has not proved to be easy to maintain the neat lines of division between contract and tort envisioned by *Moorman*. Experience has shown that certain types of claims do not fit comfortably into an "either or" dichotomy. For some claims, the answer must be "either or both," as the court recognized in *Collins v. Reynard*, 607 N.E. 2d 1185 (Ill. 1992). And this is how it should be, because the kinds of injuries recognized by the

[11] For example, in the decision of the First Circuit in *In re TJX Companies Retail Sec. Breach Litig.*, 564 F. 3d 489 (1st Cir. 2009), cited by Judge Kocoras in *Michaels Pin Pad*, the discussion of the economic loss rule consisted of three short paragraphs. And, while the court seemed to agree with the plaintiffs that they did suffer property damage because they had a property interest in their payment card information, it dismissed this argument with the conclusory statement that "[e]lectronic data can have value and the value can be lost, but the loss here is not a result of physical destruction of property." *Id.* at 498. But the court did not consider the impossibility of suffering "physical destruction" to *intangible* property, or that the requirement of physical damage as an alternative to personal injury to avoid the reach of the economic loss rule developed in the context of products liability cases, where the courts were keen to preclude expansion of strict tort liability to claims for damages to the *product* that had been purchased. *See, e.g., East River Steamship v. Transamerica*, 476 U.S. at 867(cited with approval by the Illinois Supreme Court in *Anderson Elect. v. Ledbetter Erection*, 503 N.E. 2d at 248). As relevant to this case, the "product" purchased by the consumer plaintiffs was a hotel room, the injury they allege as a result of making the purchase online had nothing at all to do with the quality of the hotel room, but their totally separate intangible property right to their personal identification and financial information. Given the prominence of products liability law in the formation of the economic loss rule, it is not too much to expect that contemporary courts applying it to the very different current commercial environment where online purchases may vastly exceed face-to-face purchases will consider whether the policies that required the application of the rule to products liability cases continue to make sense in a vastly difference electronic marketplace.

common law as compensable in tort have been broad, embracing products liability, simple negligence, negligence per se, misrepresentation and deceit, and intentional infliction of emotional injury, to name only a few.

Data security breach cases are unique in many ways. First, they are of recent origin, inasmuch as the transition to a vast digital economy has happened only recently. Second, as this case amply shows, data security breach cases do not fit neatly into the paradigm of the cases that led to the adoption of the economic loss doctrine. When a consumer logs onto the website of a hotel to book a room, the "product" purchased is a hotel room, not the secure storage of the personal and financial information required to complete the transaction. When the hotel induces the consumer to book a room online, and to hold the reservation by providing a bank card and other personal information, but fails to protect that information from hackers, the injury sustained by the consumer has nothing at all to do with the quality or fitness of the "product" purchased—the hotel room. As such, data security breach cases have very little in common with the products liability cases that launched the economic loss rule, and the policies that underlie that rule (protecting manufacturers of defective products from unlimited liability to persons they may have had no direct contact with from tort claims that the product purchased did not meet expectations) do not translate well to the circumstances of a data breach case where it simply cannot be said that the "product"—a hotel room, was in any way defective.

Moreover, what of the consumers who learn, to their dismay, that their personal information has been hacked, or that their identity has been stolen, or their credit used without authority to purchase expensive items by the hackers who stole it? As discussed above, such individuals have suffered an "injury." Yet, under the *Moorman* doctrine, however serious that injury may be, it is insufficient because it is not a "physical injury." Is this limitation justified,

given the ubiquity of the electronic marketplace and the magnitude of injuries caused by vast data breaches such as those alleged in this MDL? The Illinois Supreme Court has not had the opportunity to say.

Were the Illinois Supreme Court to consider the issues presented here, they might well agree with the conclusion reached by Judge Kocoras and the other courts that have reached the same result and find the claims barred by the economic loss rule. But the Illinois Supreme Court has shown itself to be both diligent and thoughtful in its examination of when the *Moorman* doctrine forecloses suits in tort and decline to extend the doctrine to data breach cases. Ultimately, I do not decide the issue, because, for the reasons discussed below, I find that based on the current state of Illinois law Defendants did not owe a duty to Plaintiffs to protect their personal information, notwithstanding that the Illinois Supreme Court itself has not spoken to the issue.

ii. Duty to Protect Personal Information

Defendants argue that Illinois courts do not recognize a duty to safeguard personal information, pointing to the Illinois Court of Appeals' decision in *Cooney v. Chicago Public Schools*, 943 N.E. 2d 23 (Ill. App. Ct. 2010). In that case, the Board of Education of the City of Chicago retained a graphics company to print, package, and mail a letter to 1,750 former employees to inform them that they were eligible to change their insurance benefit plans. *Id.* at 27. However, the mailing that was sent inadvertently contained the names of all 1,750 former employees, along with their "addresses, social security numbers, marital status, medical and dental insurers and health insurance plan information []." *Id.* The former employees sued, alleging, among other things, negligence under Illinois law. *Id.*

The Court of Appeals affirmed the Circuit Court's dismissal of the negligence claims, finding that the plaintiffs had not established that the Board of Education owed them a duty to

safeguard their personal information. First, the Court of Appeals found that neither the federal Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. 1320d–6(a)(3), nor the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/1 *et seq.*, created a legal duty to safeguard the plaintiffs' information. *Id.* at 28. For HIPAA, the court found that an exception regarding employee records applied to its general prohibition against disclosing personal health information. *Id.* And the court held that the plain language if IPIPA only requires data collectors that maintain personal information to "notify the owner or licensee of the information of any breach of the security of the data immediately following discovery." *Id.* (citing 815 ILCS 530/10(b)). The court rejected the plaintiffs' argument that IPIPA must also encompass a duty to protect the information from inadvertent disclosure in the first place. The court explained, "Because the provisions in the Act are clear, we must assume it reflects legislative intent to limit defendants' duty to providing notice." *Id.*

The court also declined to find a common law duty to safeguard the information. Here the court stated:

> Plaintiffs next contend that we should recognize a "new common law duty" to safeguard information. They claim a duty is justified by the sensitive nature of personal data such as dates of birth and social security numbers. Plaintiffs do not cite to an Illinois case that supports this argument. While we do not minimize the importance of protecting this information, we do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review. As noted, the legislature has specifically addressed the issue and only required the Board to provide notice of the disclosure.

Id. at 28–29. In other words, the court declined to impose a common law duty to safeguard information beyond the notice requirements of IPIPA. Accordingly, the negligence claims were dismissed. *Id.* at 29.

In *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 816 (7th Cir. 2018) the Seventh Circuit affirmed the dismissal of negligence claims in a data breach case, relying on

Cooney. That case involved a data breach at defendant Schnuck Markets, a large Midwestern grocery chain, that resulted in the theft of data for 2.4 million credit and debit cards. *Id.* at 807. The plaintiffs were a group of financial institutions that bore the costs of reissuing cards and reimbursing losses. The plaintiffs alleged common law and statutory claims against Schnuck markets, including for negligence under Illinois law. *Id.* The plaintiffs argued that Schnuck Markets had a common law duty to safeguard customers' personal information. Noting the Illinois Supreme Court had not directly spoken to this question, the Seventh Circuit followed *Cooney* and held that no common law data security duty applied. *Id.* at 816. *See also In re SuperValu, Inc.*, 925 F.3d 955, 963 (8th Cir. 2019) (dismissing Illinois negligence claim for lack of duty, explaining, "We agree with the Seventh Circuit's reading of *Cooney* and accordingly adopt its conclusion.").

Plaintiffs argue that they are not asking for a "new duty," but rather application of the general duty analysis under Illinois law. Opp. at 18. Under that analysis, Illinois courts consider "(1) the reasonable foreseeability of the injury, (2) the likelihood of the injury, (3) the magnitude of the burden of guarding against the injury, and (4) the consequences of placing that burden on the defendant." *Bruns v. City of Centralia*, 21 N.E.3d 684, 689 (Ill. 2014) (internal quotations and citations omitted). Regarding the first two prongs, Plaintiffs allege that Marriott knew or should have known that it would be the subject of a cyberattack, given that it was previously the subject of hacks, other hotel and hospitality companies were frequently the target of attacks, and the FTC issued guidance to business regarding risks of cyberattacks. Compl. ¶¶ 120; 139–65. The complaint also contains allegations that Marriott knew the Starwood data infrastructure was deficient and vulnerable to attack. Compl. ¶¶ 124–33. Regarding the third and fourth prongs, Plaintiffs allege that Marriott collects personal information for its own benefit to maximize profits,

Compl. ¶ 104., from which a court could conclude that placing the burden of reasonable security measures to guard against injury would not be unfair.

These allegations do suggest that an Illinois court could find a duty here. However, they do not escape the conclusion that any such finding would establish a "new duty" regarding data security in Illinois that *Cooney* declined to establish. Without further authority, I cannot conclude that the Illinois Supreme Court would disagree with the analysis in *Cooney*. For that reason, Plaintiffs' Illinois negligence claims are dismissed. In a future case, the Illinois Supreme Court may have the opportunity to consider this issue, along with the application of the economic loss rule to data breach cases.[12]

b. Florida Negligence Claims

Florida class representatives Lawrence, Bittner, Frakes, and Hevener allege claims of negligence under Florida Law. *See* Compl. ¶¶ 34–36; 296–304; ECF No. 368. Defendants do not dispute that Plaintiffs stated a claim for negligence under Florida law, except that Plaintiffs failed to adequately allege damages, which is an essential element of a Florida negligence claim. Def. Mot. at 31. *See Lucarelli Pizza & Deli v. Posen Const., Inc.*, 173 So. 3d 1092, 1094 (Fla. Dist. Ct. App. 2015) ("A cause of action in negligence requires proof of actual loss or damage.") For the reasons discussed below in Section V, plaintiffs have adequately alleged damages. Therefore Defendants' motion to dismiss the Florida negligence claims is denied.

c. Georgia Negligence Per Se Claims

Georgia class representatives Long, Viggiano, and Miller allege claims of negligence per se under Georgia law. *See* Compl. ¶¶ 37–39; 305–11; ECF No. 368. "It is well-settled that Georgia

[12] I am unable to certify these questions to the Illinois Supreme Court, as Illinois Supreme Court Rule 20 only allows certification of questions from the United States Supreme Court or the Seventh Circuit Court of Appeals.

law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se." *Pulte Home v. Simerly*, 746 S.E.2d 173, 179 (Ga. Ct. App. 2013). Plaintiffs base their negligence per se claim on Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 and other state statutes modeled after the FTC Act. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce." Plaintiffs argue that unfair practices, as interpreted and enforced by the FTC, include failure to use reasonable measures to protect personal information. Compl. ¶ 306. Plaintiffs allege that Marriott's failure to do so constitutes negligence per se. *Id.* at 307.

Under Georgia law, a negligence per se claim must contain an alleged "breach of a legal duty with some ascertainable standard of conduct." *Wells Fargo Bank, N.A. v. Jenkins*, 744 S.E.2d 686, 688 (Ga. 2013). To evaluate a negligence per se claim, courts must "examine the purposes of the legislation and decide (1) whether the injured person falls within the class of persons it was intended to protect and (2) whether the harm complained of was the harm it was intended to guard against." *Potts v. Fid. Fruit & Produce Co.*, 301 S.E.2d 903, 904 (Ga. Ct. App. 1983).

Several federal district courts have found that plaintiffs have adequately pled claims of Georgia negligence per se based on alleged violations of Section 5 of the FTC act in data breach cases. *See In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019); *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *14 (N.D. Ga. Mar. 5, 2018); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 2897520, at *4 (N.D. Ga. May 17, 2016); *see also First Choice Fed. Credit Union v. Wendy's Co.*, No. 16-506, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017), *report and recommendation adopted*, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017) (following *Home Depot* and declining to dismiss negligence per se claim based on Section 5 of the FTC Act).

For example, in *Home Depot*, which involved the theft of personal and financial information of 56 million Home Depot customers, the court found that "the Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect." *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 2897520, at *4. The court also explained that one Georgia case and another case applying Georgia law also suggest that the FTC Act could be the basis of a negligence per se claim. *Id.* (*citing Legacy Acad., Inc. v. Mamilove, LLC*, 328 Ga. App. 775, 790 (2014) (holding Georgia negligence per claim can be based on FTC's franchise rules interpreting Section 5 of the FTC Act), *aff'd in part and rev'd in part on other grounds*, 297 Ga. 15 (2015); *Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360-JCT, 2014 WL 637762, at *13-14 (W.D. Va. Feb. 12, 2014) (same)).

Defendants acknowledge these cases but argue that two recent Georgia Supreme Court cases suggest that the Georgia Supreme Court would find that Section 5 of the FTC Act does not create an ascertainable standard of conduct. Def. Mot. at 19–20. First, in *Wells Fargo Bank, N.A. v. Jenkins*, the plaintiff brought a negligence claim against Wachovia and related banks for allegedly giving her personal information to her husband and allowing her husband to steal her identity. 744 S.E.2d 686, 687 (Ga. 2013). Plaintiff based her negligence claim on a portion of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801(a), which provides:

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

Wells Fargo Bank, N.A. v. Jenkins, 744 S.E.2d at 687. The Georgia Supreme Court rejected this statute as a basis for a tort duty because it was a Congressional policy statement and did not require any particular duties. The court explained:

> Certainly, 15 U.S.C. § 6801(a) of the GLBA expresses the goal that financial institutions respect the privacy, security, and confidentiality of customers. While this is a clear Congressional policy statement, it is just that. It does not provide for certain duties or the performance of or refraining from any specific acts on the part of financial institutions, nor does it articulate or imply a standard of conduct or care, ordinary or otherwise. . . . Indeed, subsection (b) of 15 U.S.C. § 6801 confirms that subsection (a) is not intended to provide a standard of conduct or care by financial institutions as it expressly authorizes federal agencies "[i]n furtherance of the policy in subsection (a) [of § 6801]" to: establish appropriate standards for the financial institutions . . . ."

Wells Fargo Bank, N.A. v. Jenkins, 744 S.E.2d at 688.

Second, in *Dep't of Labor v. McConnell*, the Georgia Supreme Court affirmed the dismissal of negligence per se claims brought under two Georgia statutes. 828 S.E.2d 352, 356 (2019). In that case, Defendant Georgia Department of Labor inadvertently sent an email to 1,000 recipients that included a spreadsheet containing the "name, social security number, home telephone number, email address, and age of 4,757 individuals . . . who had applied for unemployment benefits or other services administered by the Department" including the named plaintiff. The plaintiff alleged that two Georgia statutes, OCGA §§ 10-1-910 and 10-1-393.8, "created a legal duty on the part of the Department to safeguard his and the other proposed class members' personal information." *Id.* at 358. OCGA §§ 10-1-910, titled "Legislative findings," states:

> The General Assembly finds and declares as follows:
>
> (1) The privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors;
>
> (2) Credit card transactions, magazine subscriptions, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet

> websites are all sources of personal information and form the source material for identity thieves;
>
> (3) Identity theft is one of the fastest growing crimes committed in this state. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, purchase property, and commit other financial crimes with other people's identities;
>
> (4) Implementation of technology security plans and security software as part of an information security policy may provide protection to consumers and the general public from identity thieves;
>
> (5) Information brokers should clearly define the standards for authorized users of its data so that a breach by an unauthorized user is easily identifiable;
>
> (6) Identity theft is costly to the marketplace and to consumers; and
>
> (7) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative.

Ga. Code Ann. § 10-1-910. The Georgia Supreme Court held that this statute did not form a basis for plaintiff's negligence claim, because it "does not explicitly establish any duty, nor does it prohibit or require any conduct at all. Rather, the statute recites a series of legislative findings about the vulnerability of personal information and the risk of identity theft." *Dep't of Labor v. McConnell*, 828 S.E.2d at 358.

The other statute cited in *McConnell* as a basis for a duty, OCGA § 10-1-393.8, states in relevant part:

> (a) Except as otherwise provided in this Code section, a person, firm, or corporation shall not:
>
> (1) Publicly post or publicly display in any manner an individual's social security number. As used in this Code section, "publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public;
>
> (2) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted; or

> (3) Require an individual to use his or her social security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.

Ga. Code Ann. § 10-1-393.8. The Georgia Supreme Court rejected this as a basis for a negligence claim as well, holding that even if this section did create an enforceable duty, the text of the statute only applies to *intentional* disclosures of information, and the plaintiff only alleged negligent disclosure. *Id.*[13]

Defendant argues that the reasoning of these cases indicates that the Georgia Supreme Court would decline to find Section 5 of the FTC Act creates an enforceable duty. But unlike the statement of policy in *Wells Fargo Bank* and the legislative findings in *McConnell*, Section 5 of the FTC Act *is* a statute that creates enforceable duties. Moreover, this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context.

For example, in *F.T.C. v. Wyndham Worldwide Corp.*, the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases, which it had been doing since 2005. 799 F.3d 236, 240 (3d Cir. 2015) ("The Federal Trade Commission Act prohibits 'unfair or deceptive acts or practices in or affecting commerce.' 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with

[13] Defendants also argue that *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 817 (7th Cir. 2018) casts doubt on the validity of the *Home Depot* decision. In that case, the Seventh Circuit said that the Court of Appeals of Georgia disagreed with the *Home Depot* prediction of state law, citing the Georgia Court of Appeals opinion in *McConell* that was vacated on other grounds by the Georgia Supreme Court in the *McConnell* decision discussed above. But the Georgia Court of Appeals in *McConnell* did not disagree with the *Home Depot* court's finding that Section 5 of the FTC Act could form the basis for a negligence per se action, which is the question here. Rather, the intermediate *McConnell* court declined to extend the *Home Depot* court's holding that defendants owed a duty to safeguard personal information based on the more general duty owed to the world not to subject others to an unreasonable risk of harm to the facts before it. *See McConnell*, 787 S.E.2d 794, 797 n.4 (Ga. App. 2016).

allegedly deficient cybersecurity that failed to protect consumer data against hackers.") In that case, Wyndham Worldwide, a hotel and hospitality company, was the subject of multiple cyberattacks that compromised the personal information of hundreds of thousands of its customers. *Id.* The FTC brought an administrative action against Wyndham for inadequate cybersecurity practices. Wyndham challenged the authority for the FTC to do so, but the FTC's enforcement action was affirmed by both a New Jersey District Court and the Third Circuit. *Id.* at 259.

The Third Circuit first found that the allegations regarding Wyndham's cybersecurity practices, including that it had an allegedly misleading privacy policy that overstated its cybersecurity, fell within the plain meaning of "unfair" practices in the text of Section 5 of the FTC Act. *Id.* at 246–47. Further, the court held that Wyndham had fair notice that its conduct could fall within the meaning of the statute based on a "cost-benefit analysis that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." *Id.* at 255 (internal citations omitted). Considering the alleged deficiency of Wyndham's cybersecurity practices, the court found that they had fair notice that their conduct could violate the FTC Act. This conclusion was reinforced by an FTC guidebook published in 2007 titled, *Protecting Personal Information: A Guide for Business*, that provides recommendations on cybersecurity practices, and FTC complaints and consent decrees in administrative cases raising unfairness claims based on inadequate cybersecurity practices, all of which provided additional notice to Wyndham regarding their duties and a potential enforcement action. *Id.* at 255–57.[14] S*ee also In re TJX Companies Retail Sec.*

[14] Plaintiffs here also point to the FTC guidebook, *Protecting Personal Information: A Guide for Business*, as evidence that Marriott failed to comply with regulatory guidance. *See* Compl. ¶¶ 256–61.

Breach Litig., 564 F.3d 489, 498–99 (1st Cir. 2009), *as amended on reh'g in part* (May 5, 2009) (applying FTC precedent for scope of duty under Massachusetts law based on Section 5 of FTC act).

Therefore, based on the Georgia appellate court decisions finding negligence per se based on rules interpreting Section 5 of the FTC Act, and the aforementioned federal district court decisions finding negligence per se based on the Section 5 FTC Act in data breach cases, I am persuaded that Plaintiffs have adequately pled negligence per se under Georgia law. Defendants' motion to dismiss these claims is denied.

III. Contract Claims

Bellwether Plaintiffs allege breach of express contract under the laws of New York and Maryland, and breach of implied contract based on Oregon law. Defendants move to dismiss each claim. For the reasons discussed below, Defendants' motion to dismiss the contract claims is denied.

a. New York and Maryland Express Contract Claims

New York class representatives Cullen, Fishon, and O'Brien, and Maryland Class Representatives Maldini and Ryans allege breach of express contract claims. *See* Compl. ¶¶ 52–53, 70–72, 312–28; ECF No. 368. These claims are based on alleged contracts formed by Marriott and Starwood's privacy statements that were in effect at the time of the breach.

Both Maryland and New York apply the objective standard for the formation of contracts, which looks to objective manifestations of intent. *See Address v. Millstone*, 56 A.3d 323, 335 (Md. Ct. Spec. App. 2012) ("Maryland . . . applies the objective standard as to the formation of contracts") (internal citation omitted); *Brighton Inv., Ltd. v. Har-ZVI*, 932 N.Y.S.2d 214, 216 (N.Y. App. Div. 2011) ("Whether a contract has been formed does not depend on either party's subjective

intent; instead, the determination must be based on 'the objective manifestations of the intent of the parties as gathered by their expressed words and deeds'") (internal citation omitted).

Plaintiffs allege that Marriott's privacy statement dated May 18, 2018 provides that individuals are subject to its terms and conditions when they do the following: "(1) log onto Marriott's website; (2) use Marriott's software applications; (3) access Marriott's social media pages; (4) receive e-mail communications from Marriott that link to the Privacy Statement; and (5) 'when you visit or stay as a guest at one of [Marriott's] properties, or through other offline interactions.'" Compl. ¶ 314. Further, Plaintiffs allege that Marriott's Privacy Statement provides that: "Collectively, we refer to the Websites, the Apps and our Social Media Pages, as the 'Online Services' and, together with offline channels, the 'Services.' ***By using the Services, you agree to the terms and conditions of this Privacy Statement.***" *Id.* (emphasis in Compl.). Regarding the terms of the Privacy Statement, Plaintiffs allege that the Marriott Privacy Statement provides that Marriott would use "reasonable organizational, technical and administrative measures to protect [its customers'] Personal Data." *Id.* at ¶ 317.

Likewise, Plaintiffs allege that Starwood's privacy statement dated October 14, 2014 provides that individuals are subject to its terms and conditions when they do the following: "(1) make reservations or submit information requests to Starwood; (2) purchase products or services from Starwood; (3) register for Starwood program membership; and (4) respond to communications from Starwood." Compl. ¶ 319. As to the terms, Plaintiff alleges that the Starwood Privacy Statement provides the following:

> Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. . . .

> [Starwood] safeguard[s] your information using appropriate administrative, procedural and technical safeguards, including password controls, 'firewalls' and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit. . . .
>
> By becoming a member of the SPG Program (an 'SPG Member') and receiving and redeeming benefits of the SPG Program including, without limitation, Starpoints®, each SPG Member agrees that he/she has . . . provided consent for Starwood, the SPG Participating Hotels and their authorized third party agents to process data that is personal to him/her, and to disclose such data to third parties, in accordance with Starwood's Privacy Statement.

Compl. ¶¶ 320–22. All Bellwether Plaintiffs alleged that they provided their personal information to stay at a Marriott property before the data breach, and Plaintiff Cullen alleges that he had an SPG payment card. *See* Compl. ¶¶ 25–28, 34–39, 42–43, 52–53, 55–56, 70–72, 77. Plaintiffs argue that these allegations sufficiently establish the formation of a contract for data security.

Defendants argue that these pleadings fail to allege formation of a contract because Plaintiffs do not specifically allege that they read, saw, or understood the Privacy Statements. To support its position, Defendants point to several cases that found company privacy statements did not give rise to an enforceable contract. For example, in *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1199–1200 (D.N.D. 2004), the court concluded:

> Having carefully reviewed the complaint, the Court finds the Plaintiffs' breach of contract claim fails as a matter of law. First, broad statements of company policy do not generally give rise to contract claims. *See Pratt v. Heartview Foundation*, 512 N.W.2d 675, 677 (N.D. 1994); *accord Martens v. Minnesota Mining and Manu. Co.*, 616 N.W.2d 732, 740 (Minn. 2000). As such, the alleged violation of the privacy policy at issue does not give rise to a contract claim. Second, nowhere in the complaint are the Plaintiffs alleged to have ever logged onto Northwest Airlines' website and accessed, read, understood, actually relied upon, or otherwise considered Northwest Airlines' privacy policy.

See also Gardner v. Health Net, Inc., 2010 WL 11597979, at *6 (C.D. Cal. Aug. 12, 2010) ("Plaintiffs have failed to allege that they ever submitted any information over Defendant's

website, accessed or read the Privacy Policy, or relied on the Privacy Policy. As noted by the court in *Dyer*, such allegations are insufficient because 'broad statements of policy do not generally give rise to contract claims.' 334 F.Supp.2d at 1199–1200."). Other cases have placed an emphasis on reliance to plausibly state a claim. *See Azeltine v. Bank of Am.*, 2010 WL 6511710, at *10 (D. Ariz. Dec. 14, 2010) ("In contrast to *Dyer*, 334 F. Supp. 2d at 1200, which held that a general statement of company policies, like a privacy policy, did not give rise to a contract claims, other courts have stated that, on a motion to dismiss, a court's inquiry should be whether it is plausible that the policy or statement constituted a contract. . . . In conducting this inquiry, the court should determine whether the plaintiff has alleged that he has relied on the policy.")

Here we must look to the parties' objective manifestations of intent. Marriott and Starwood's Privacy Statements, which by their own terms apply to guests that stay at Marriott and Starwood properties or enroll in the SPG Program, constitute objective offers to protect the personal information that it collects under the terms of the privacy statements. Plaintiffs' allegations that they assented to these offers by staying at Marriott and Starwood properties, enrolling in the SPG Program, and providing their personal information to Marriott and Starwood constitute objective manifestations of acceptance of Defendants' offers. Indeed, this is all that the privacy statements themselves require in order to be binding on consumers. Thus plaintiffs have adequately alleged formation of a contract.

Defendants also argue that the Complaint does not include dates for when each plaintiff stayed at a Marriott hotel, or which Marriott entity they stayed with, and therefore the Plaintiffs did not sufficiently plead that they were party to a contract. These are matters for discovery. All plaintiffs have alleged that they stayed at a Marriott property before the data breach, that they gave

their personal information as a manifestation of intent to accept the terms of the privacy statements, and that the privacy statements were in effect during this time. That is enough to state a claim.

Finally, Defendants argue that the contract terms are not sufficiently definite to make out a contract for data security. I disagree. The Marriott Privacy Statement provides that it will use "reasonable organizational, technical and administrative measures to protect [its customers'] Personal Data." Compl. ¶ 317. And the Starwood Privacy Statement says that it will "safeguard your information using appropriate administrative, procedural and technical safeguards," and provides detailed examples of the methods it will use. Compl. ¶ 320–22. While the parties may dispute the contours of these duties and whether they were breached after discovery, at this stage Plaintiffs have plausibly alleged the terms of the contract regarding data security.

Therefore, for the reasons stated above, Plaintiffs have plausibly stated claims for breach of contract under New York and Maryland law. Defendants' motion to dismiss these claims is denied.

b. Oregon Implied Contract Claim

Oregon class representative Ropp alleges breach of implied contract. *See* Compl. ¶ 77, 329–36; ECF No. 368. Under Oregon law, in "an implied-in-fact contract, the parties' agreement is inferred, in whole or in part, from their conduct." *Larisa's Home Care, LLC v. Nichols-Shields*, 404 P.3d 912, 919 n.5 (Or. 2017) (*citing Restatement (Second) of Contracts* § 4 comment a (1979)). "[A] contract implied in fact can arise 'where the natural and just interpretation of the acts of the parties warrants such conclusion.'" *Id.* (*quoting Owen v. Bradley*, 371 P.2d 966 (Or. 1962)). "[A]n implied-in-fact contract, 'like any other contract, must be founded upon the mutual agreement and intention of the parties.'" *Mindful Insights, LLC v. VerifyValid, LLC*, 454 P.3d 787,

793 (Or. Ct. App. 2019) (quoting *Rose v. Wollenberg*, 59 P. 190, 191 (Or. 1899)). Oregon courts distinguish between implied-in-fact and express contracts as follows:

> When an agreement consists of words, written or spoken, stating in terms the understanding and obligations of the parties, it is called an 'express contract'; but when it is inferred from the acts or conduct of the parties, instead of their words, it is an 'implied contract.' But in either instance it exists as an obligation solely because the contracting party has willed, under circumstances to which the law attaches the sanction of an obligation, that he shall be bound. And the distinction between an express and implied contract lies, not in the nature of the undertaking, but solely in the mode of proof. In either case there must be an offer of terms, or its equivalent, on the one side, and the acceptance of such terms, or its equivalent, on the other. When this intention is expressed, we call the contract an express one. When it is not expressed, it may be inferred, implied, or presumed, from circumstances as really existing, and then the contract, thus ascertained, is called an implied one.

Id. (quoting *Rose v. Wollenberg*, 59 P. at 191) (internal citation and quotation marks omitted in original.)

For example, in *Otterness v. City of Waldport*, a case cited by Defendants, the Oregon Court of Appeals rejected an implied contract claim where plaintiffs alleged that they applied and paid the fee for a building, and that as a consequence the city building department had implied duties to inspect and certify the building under the laws of Oregon. 883 P.2d 228, 229 (Or. Ct. App. 1994). The court found that there was "a complete absence of allegations describing the 'acts of the parties' that warrant the conclusion that a contract was intended" as there were "no allegations as to anyone's acts in plaintiffs' complaint, beyond plaintiffs' payment of $608.60 to defendant to process its application." *Id.* at 232 (internal citation omitted). Thus the court affirmed the dismissal of the implied contract claim. In contrast, in *Yoshida's Inc. v. Dunn Carney Allen Higgins & Tongue LLP*, the Oregon Court of Appeals found that a reasonable jury could find an implied contract in a case against a law firm for failing to provide plaintiffs with requested documents. 356 P.3d 121, 135 (Or. Ct. App. 2015). The court based this conclusion on the "course

of conduct" of the parties, specifically that plaintiffs said that they wanted the work to be done "ASAP," provided defendants with a billing code, and defendants began performing the work. *Id.*

The parties do not cite, and I have not found, any Oregon cases analyzing implied contract claims in a data breach case. Instead, Defendants point to data breach cases in which the courts have dismissed implied contract claims based on Washington law. *See Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010); *Lovell v. P.F. Chang's China Bistro, Inc.*, 2015 WL 4940371, at *3 (W.D. Wash. Mar. 27, 2015). Plaintiffs cite to cases applying California, Colorado, and Maine law that have not dismissed implied contract claims. *See Castillo v. Seagate Tech., LLC*, Case No. 16-cv-01958-RS, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016); *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1247–48 (D. Colo. 2018); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 119 (D. Me. 2009), *aff'd in relevant part, Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011); *Rudolph v. Hudson's Bay Co.*, No. 18-CV-8472 (PKC), 2019 WL 2023713, at *11 (S.D.N.Y. May 7, 2019).

Applying the principles of implied contract under Oregon law outlined above, Plaintiff Ropp has sufficiently alleged breach of implied contract. Ropp makes the same allegations as the New York and Maryland plaintiffs regarding Marriott and Starwood's privacy statements. And Ropp alleges that he "provided his Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach [and] . . . also provided his passport information in order to stay at a Marriott Property." Compl. ¶ 77. These alleged actions plausibly state a way for Ropp to manifest his assent to the privacy statements. After discovery, the parties may dispute whether Ropp or other plaintiffs' alleged contract claims are properly considered express or implied contracts, but at this stage both have been sufficiently pled. *See Mindful Insights, LLC v. VerifyValid, LLC*, 454 P.3d at 795 ("[B]reach of express contract and breach of implied-in-fact

contract are not distinct claims but instead involve alternative ways of proving how the parties manifested their agreement—either orally or in writing (express) or through conduct (implied-in-fact). They are no different in legal effect.") Therefore, Defendants' motion to dismiss the Oregon implied contract claim is denied.

IV. Statutory Claims

Bellwether Plaintiffs allege breach of statutory duties under the laws of Maryland, Michigan, California and New York. Defendants move to dismiss each claim. For the reasons discussed below, Defendants' motion to dismiss the statutory claims is denied.

a. Maryland Personal Information Privacy Act Claims

Maryland Class Representatives Maldini and Ryans allege violations of the Maryland Personal Information Privacy Act ("PIPA"), Md. Comm. Code §§ 14-3501, *et seq*. *See* Compl. ¶¶ 52–53,355–68; ECF No. 368.[15] In relevant part, PIPA states:

> To protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations.

Md. Comm. Code § 14-3503(a). Thus, the plain language of PIPA requires businesses to implement and maintain "reasonable security practices and procedures" based on the personal information they collect. "Personal Information" is defined to include "[a]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another

[15] Marriott selected the Maryland Consumer Protection Act claims as a bellwether claim for the purposes of this motion to dismiss. *See* ECF No. 368. Plaintiffs allege that one of the ways that Defendants violated the Maryland Consumer Protection Act claim is by violating the Maryland PIPA. Therefore, although the Maryland PIPA claim was not selected separately as a bellwether claim, I address it here for clarity before turning to the Maryland Consumer Protection Act claim below.

method that renders the information unreadable or unusable: . . . a passport number . . . [a]n account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account." Md. Comm. Code § 14-3503(e)(1). Further, PIPA requires a business that has discovered or has been notified of a security breach to conduct a prompt investigation to determine if Personal Information has or will be misused. Md. Comm. Code § 14-3504(b)(1). If so, "the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system." Md. Comm. Code §§ 14-3504(b)(2), 14-3504(c)(2).

Here Plaintiffs allege that Marriott did not maintain reasonable security measures appropriate to the nature of their Personal Information as required by PIPA. Compl. ¶ 360. Plaintiffs support this allegation with a detailed summary of the breach and alleged failings to secure personal information. *See, e.g.*, Compl. ¶ 227 ("A company with proper information security would not have allowed outsiders to have access to such a massive variety of information systems over four years even if they somehow managed to access internal systems for a brief period of time.") Plaintiffs also allege that Marriott did not provide timely notice of its data breach as required by PIPA. Compl. ¶ 365. In this regard, Plaintiffs allege that Marriott waited more than two months to inform guests after it received notice of the breach. *See* Compl. ¶¶ 178, 187, 194.

Defendants argue that Plaintiffs Maldini and Ryans failed to state a claim under PIPA because the statute covers only unencrypted payment card numbers when they are accompanied

by access or security codes, and that Plaintiffs did not allege that any such codes or passwords were implicated in the cyberattack.[16] Def. Mot. 28.

Plaintiffs respond that this does not defeat their claims because they do not allege that any codes were "required" to allow fraudulent use of their personal information. Plaintiffs point to the fraudulent charges of some plaintiffs, which Defendants do not dispute at this stage, as evidence of this. Further, Plaintiffs argue that although Marriott has not publicly disclosed that security codes were compromised, the full scope of the data breach is not yet known. In this regard, Plaintiffs specifically allege that hackers likely had access to "full payment card information with encryption keys," a possibility that experts could not rule out after Marriott's investigation. Compl. ¶ 208; *see also id.* ¶ 2 ("The stolen information includes . . . tools needed to decrypt cardholder data. . . . Marriott has been unable to definitively determine how much data was stolen . . .") and ¶¶ 189–190, 197, 234. And in at least one initial report, Starwood indicated that security codes were compromised. *See* Compl. ¶ 146 ("In a letter to Starwood customers, Starwood stated that the 'malware was designed to collect certain payment card information, including cardholder name, payment card number, security code and expiration date'").

Plaintiffs have sufficiently alleged PIPA violations for two independent reasons. First, Plaintiffs have plausibly alleged that Marriott failed to employ reasonable security measures to protect the Personal Information it collected. Plaintiffs provide numerous allegations to support this claim. Here I do not need to resolve whether security codes must be compromised as a matter

[16] Although passports are also included under PIPA's definition of Personal Information, Defendants argue that Plaintiffs Maldini and Ryans are not among those Plaintiffs that allege their passport information was stolen. Plaintiffs argue that Maldini and Ryans can nonetheless represent Maryland class members whose passports were stolen. Because I find that Maldini and Ryans have adequately stated a PIPA claim based on the allegations above, I need not resolve this question.

of law to state a PIPA claim, because Plaintiffs allege that such codes likely were compromised in the data breach and I must grant all inferences in favor of Plaintiffs. Therefore Plaintiffs have adequately alleged a PIPA claim.

Second, Plaintiffs have plausibly alleged that Marriott's failure to disclose the data breach for more than two months was a violation of PIPA's requirement to provide timely notice to consumers affected by a data breach. Further discovery may establish that Marriott did act reasonably promptly, or that it did not. Either way, Plaintiffs have stated enough facts to allow the claim to go forward.

b. Maryland Consumer Protection Act Claims

Maryland class representatives Maldini and Ryans also allege violations of the Maryland Consumer Protection Act ("CPA"), Md. Comm. Code §§ 13-301, *et seq*. *See* Compl. ¶¶ 52–53, 369–82; ECF No. 368. The CPA prohibits "unfair or deceptive trade practices" which include:

> False, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers; . . .
>
> Representation that: Consumer goods, consumer realty, or consumer services have a sponsorship, approval, accessory, characteristic, ingredient, use, benefit, or quantity which they do not have; . . .
>
> Failure to state a material fact if the failure deceives or tends to deceive; . . .
>
> Advertisement or offer of consumer goods, consumer realty, or consumer services . . . [w]ithout intent to sell, lease, or rent them as advertised or offered; . . .
>
> Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with: [t]he promotion or sale of any consumer goods . . . or consumer service; . . . [or] [t]he subsequent performance of a merchant with respect to an agreement of sale, lease, or rental; . . .

Md. Comm. Code § 13-301. In addition, a violation of the Maryland PIPA constitutes a violation of the Maryland CPA. *See* Md. Comm. Code § 14-3508 ("A violation of [subtitle 35: Maryland

Personal Information Protection Act]: (1) Is an unfair or deceptive trade practice within the meaning of Title 13 of this article; and (2) Is subject to the enforcement and penalty provisions contained in Title 13 of this article.")

Plaintiffs allege that Marriott engaged in unfair and deceptive trade practices based on its material representations and omissions regarding its data security. Compl. ¶ 376. In addition, Plaintiff's incorporate their arguments regarding the alleged violation of PIPA as a basis for a violation under the CPA. *Id.*

Defendants argue that Plaintiffs' CPA claims fail because they do not allege that they were aware of any representation from Marriott or Starwood about data security. Def. Mot. at 27. In addition, Defendants argue that a CPA claim is subject to the heightened pleading requirement of Federal Rule of Civil Procedure 9(b) because it sounds in fraud, and that Plaintiffs have failed to allege their claims with sufficient particularity. *Id.* Finally, Defendants incorporate their arguments discussed above regarding the PIPA claims. *Id.* at 28.

Plaintiffs have sufficiently alleged a violation of the Maryland CPA for two independent reasons. First, as discussed above, Plaintiffs have adequately pled a violation of the Maryland PIPA. Because this constitutes an "unfair or deceptive trade practice" for purposes of Title 13 of the Maryland Commercial Law Code, it provides a sufficient basis for Plaintiffs' CPA claims.

Second, Plaintiffs have met the requirements of Rule 9(b), including with regard to their allegations of reliance on material omissions by Defendants. Rule 9(b) requires the Plaintiffs to allege "the time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby." *Harrison v. Westinghouse Savannah River Co.*, 176 F.3d 776, 784 (4th Cir. 1999) (internal quotation marks omitted). But where a claim of fraud is based on an omission, meeting Rule 9(b)'s particularity requirement

takes a different form. *Lombel v. Flagstar Bank F.S.B.*, No. PWG-13-704, 2013 WL 5604543, at *6 (D. Md. Oct. 11, 2013); *Willis v. Bank of Am. Corp.*, No. ELH-13-02615, 2014 WL 3829520, at *8 (D. Md. Aug. 1, 2014) ("Rule 9(b) is 'less strictly applied with respect to claims of fraud by concealment' or omission of material facts, as opposed to affirmative misrepresentations, because 'an omission cannot be described in terms of the time, place, and contents of the misrepresentation or the identity of the person making the misrepresentation.') (quoting *Shaw v. Brown & Williamson Tobacco Corp.*, 973 F. Supp. 539, 552 (D. Md. 1997)). "'[A] consumer relies on a material omission under the [Maryland CPA] where it is substantially likely that the consumer would not have made the choice in question had the commercial entity disclosed the omitted information.'" *Willis v. Bank of Am. Corp.*, 2014 WL 3829520, at *22 (quoting *Bank of Am., N.A. v. Jill P. Mitchell Living Trust*, 822 F. Supp. 2d 505, 535 (D. Md. 2011)).

Here the Complaint contains extensive allegations that Marriott knew or should have known about its allegedly inadequate data security practices and the risk of a data breach. *See, e.g.*, Compl. ¶¶ 115–28 (reviewing Marriott's alleged "lack of cybersecurity due diligence"); ¶ 139 (alleging Marriott and Starwood knew they were prime targets for hackers and had been the target of cyberattacks); ¶¶ 256–60 (alleging failure to follow FTC guidelines to reduce risk of cyberattack). Plaintiffs also allege that these omissions would have been important to a significant number of consumers, that Plaintiffs relied on the omissions, and that Plaintiffs "would not have paid Marriott for goods and services or would have paid less for such goods and services" if it had known the truth about Marriott's alleged omissions. Compl. ¶¶ 377, 379, 381. These allegations establish that "it is substantially likely that the consumer would not have made the choice in question had the commercial entity disclosed the omitted information." *Willis v. Bank of Am. Corp.*, 2014 WL 3829520, at *22 (internal quotation marks omitted). Therefore Plaintiffs have

met the particularity requirements of Rule 9(b) and sufficiently alleged reliance on Defendants material omissions.

Thus Plaintiffs have adequately alleged violations of the Maryland CPA. Defendants' motion to dismiss these claims is denied.

c. Michigan Identity Theft Protection Act Claims

Michigan class representatives Wallace and Gononian allege claims under the Michigan Identity Theft Protection Act ("ITPA"), Mich. Comp. Laws §§ 445, *et seq.* *See* Compl. ¶¶ 55–56, 778–85; ECF No. 368. The ITPA requires businesses to provide notice of a security breach "without unreasonable delay" to a Michigan resident if that resident's unencrypted and unredacted "personal information" was accessed by an unauthorized person. Mich. Comp. Laws § 445.72(1). "Personal information" is defined as a person's "first name or first initial and last name" linked to one or more data elements including a "credit or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts." *Id.* at § 445.63(r). The ITPA notice provision applies when the business discovers a security breach or receives notice of a security breach, unless the breach is not likely to cause harm. *Id.* at § 445.72(1).

Plaintiffs claim that Defendants failed to disclose the cyberattack in a timely and accurate fashion. Compl. ¶ 783. As described above, Plaintiffs allege that Defendants waited more than two months after they had notice of the breach to disclose it to guests. *See* Compl. ¶¶ 178, 187, 194. Defendants argue that this claim should be dismissed for the same reason as the Maryland PIPA claim, specifically that the statute only applies to payment card numbers combined with security codes, and that Plaintiffs do not allege security codes were taken. Def. Mot. at 28.

For the reasons discussed above regarding the Maryland PIPA claim, Defendants' argument is unavailing. Plaintiffs do not allege that any information was required to access their financial accounts, and indeed Defendants do not dispute that some Plaintiffs allege fraudulent charges. Moreover, Plaintiffs have alleged that security codes were likely obtained by hackers and that Marriott does not yet know the full extent of the data breach. These allegations are sufficient to state a claim under the ITPA. The full scope of the data breach is a matter for discovery. Thus, Defendants' motion to dismiss the Michigan ITPA claims is denied.

d. California Unfair Competition Law Claims

California class representatives Guzikowski, Marks, Sempre, and Maisto allege claims under the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.* *See* Compl. ¶¶ 25–28; 450–59; ECF No. 368. The California UCL prohibits unfair competition including "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

Plaintiffs allege that Marriott violated the UCL by failing to implement and maintain reasonable security measures to protect their personal information, failing to comply with common law and statutory duties regarding data protection including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law, misrepresenting that it would comply with these statutory obligations and protect the privacy and confidentiality of Plaintiffs' personal information, and concealing the material fact that it did not reasonably secure Plaintiffs' personal information or comply with statutory duties. Compl. ¶ 455.

Defendants move to dismiss these claims, arguing that they have not been pled with particularity as required by Rule 9(b) and that Plaintiffs lack standing under the statutory requirements of the UCL. Defendants' motion to dismiss these claims is denied.

First, for the same reasons discussed above regarding the Maryland CPA claim, Plaintiffs have met the Rule 9(b) pleading requirements for their California UCL claim. In short, the Complaint contains extensive allegations that Marriott knew or should have known about its allegedly inadequate data security practices and the risk of a data breach and that its alleged failures and omissions were material and relied upon by consumers. *See, e.g.*, Compl. ¶¶ 115–28, 256–60, 377, 379, 381.

Second, Plaintiffs have sufficiently alleged UCL standing. Standing to state a claim under the UCL is limited to "any 'person who has suffered injury in fact and has lost money or property' as a result of unfair competition." *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 884 (Cal. 2011) (quoting Cal. Bus. & Prof. Code § 17204, as amended by Prop. 64, as approved by voters, Gen. Elec. (Nov. 2, 2004)). In other words, to have standing to state a UCL claim, a person "must demonstrate some form of economic injury." *Id.* This can be shown in multiple ways, including the following:

> A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.

Kwikset Corp, 246 P.3d 877 at 885–86.

Defendants point to several data breach cases in which courts have dismissed UCL claims. For example, in *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, a case arising out of the Starwood data breach, the plaintiff alleged that unauthorized charges were made on his credit card, that he would incur damages to monitor identity theft, and that he spent time responding to

unauthorized charges on his credit card. No. 316CV00014GPCBLM, 2016 WL 6523428, at *11 (S.D. Cal. Nov. 3, 2016). The court held that these allegations did not suffice to establish standing for the UCL claims because the plaintiff did not allege any unreimbursed losses. *Id.* at *4, *11. The court also said that the plaintiff failed to establish that loss of his personal information constitutes a form of property loss for the UCL. *Id.* at *6, *11. *See also Gardner v. Health Net, Inc.*, No. CV 10-2140 PA (CWX), 2010 WL 11597979, at *12 (C.D. Cal. Aug. 12, 2010) (holding plaintiff failed to establish UCL standing where plaintiff alleged time and expense monitoring credit and loss of value of personal information but Defendant had offered credit monitoring services); *Ruiz v. Gap, Inc.*, No. 07-5739 SC, 2009 WL 250481, at *3 (N.D. Cal. Feb. 3, 2009) (denying motion to amend complaint to add UCL claims, because plaintiff could not establish UCL standing based on costs associated with monitoring credit and loss of value of personal information where defendant offered credit monitoring services), *aff'd*, 380 F. App'x 689 (9th Cir. 2010).

But other courts have reached the exact opposite conclusion and denied motions to dismiss UCL claims in data breach cases. For example, in *In re Anthem, Inc. Data Breach Litigation*, Judge Koh found that the plaintiffs' allegations that they lost the benefit of their bargain was sufficient to satisfy the economic injury requirement for standing under the UCL, explaining that this type of loss "mirrors the California Supreme Court's determination in *Kwikset* that a plaintiff who has 'surrender[ed] in a transaction more, or acquire[d] in a transaction less, than he or she otherwise would have' may bring a UCL claim." 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016) (quoting *Kwikset*, 246 P.3d at 885); *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014) (holding plaintiffs had UCL standing where "[f]our of the six Plaintiffs allege they personally spent more on Adobe products than they would had they known

Adobe was not providing the reasonable security Adobe represented it was providing"); *In re LinkedIn User Privacy Litig.*, No. 12-cv-3088-EJD, 2014 WL 1323713, *4 (N.D. Cal. Mar. 28, 2014) (holding benefit-of-the-bargain losses "sufficient to confer . . . statutory standing under the UCL.")

Here, like the plaintiffs in *Anthem, Adobe*, and *LinkedIn*, Plaintiffs have sufficiently alleged benefit-of-the-bargain losses. *See* Section I.a.iv above. In short, Plaintiffs allege that "had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their data—they would not have stayed at a Marriott Property, purchased products or services at a Marriott Property, and/or would have paid less." Compl. ¶ 275. This is sufficient to establish standing for the UCL claim. *See Kwikset*, 246 P.3d at 885–86 (economic injury established where plaintiff "surrender[s] in a transaction more, or acquire[s] in a transaction less, than he or she otherwise would have"). Moreover, Plaintiffs Guzikowski and Sempre claim they spent money purchasing credit-monitoring and identity-theft services to mitigate the damages from the breach. Compl. ¶¶ 25, 27. Unlike in *Dugas*, *Gardner*, and *Ruiz*, the pleadings do not indicate that these expenses have been reimbursed. Therefore these payments also constitute economic injury. *See Kwikset*, 246 P.3d at 885–86 (economic injury established where plaintiff is "required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.")[17]

Accordingly, Defendants' motion to dismiss the California UCL claims is denied.

[17] Plaintiffs may also have established standing to state their UCL claims based on the loss of property value of their personal information. *See* Section I.a.iii *supra*; *Kwikset*, 246 P.3d 877, 885–86 (2011) (economic injury established where plaintiffs "have a present or future property interest diminished"). But because the parties did not brief the issue of whether California courts would recognize the loss of value of personal information as an economic injury, I do not decide that question here.

e. New York General Business Law Claims

New York class representatives Cullen, Fishon, and O'Brien allege claims under the New York General Business Law ("GBL"), N.Y. Gen. Bus. §§ 349, *et seq*. *See* Compl. ¶ 70–72, 934–42; ECF No. 368. Section 349(a) of the GBL prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service." N.Y. Gen. Bus. § 349(a). To state a § 349 GBL claim, plaintiff must allege (1) that defendant's "act or practice was consumer-oriented," (2) that the act or practice "was misleading in a material way," and (3) that plaintiff "suffered injury as a result of the deceptive act." *Stutman v. Chem. Bank*, 731 N.E.2d 608, 611 (N.Y. 2000). "[T]o qualify as a prohibited act under the statute, the deception of a consumer must occur in New York." *Goshen v. Mut. Life Ins. Co. of New York*, 774 N.E.2d 1190, 1195 (N.Y. 2002).

Each of the New York class representatives alleges that he or she "is a resident of New York and provided [his or her] Personal Information to Marriott in order to stay at a Marriott Property prior to the Data Breach." Compl. ¶¶ 70–72. The New York class representatives and members of the New York Subclass also allege that they "were deceived in New York" and "transacted with Marriott in New York by making hotel reservations from New York and/or staying in Marriott properties based in New York." Compl. ¶ 936. Plaintiffs allege that Marriott's deceptive acts or practices include failing to implement and maintain reasonable security and privacy measures, failing to identify and remediate foreseeable privacy risks, failing to comply with statutory duties regarding the security and privacy of Plaintiffs' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, misrepresenting that it would protect the Plaintiffs' personal information, and concealing its failure to take reasonable measures or comply with statutory and common law duties to do so. Compl. ¶ 935. Plaintiffs claim that these

acts affected the public interest and consumers at large, and the New York class representatives and New York class members suffered damages as a result of Marriott's alleged practices. Compl. ¶ 939–40.

Defendants move to dismiss these claims, arguing that Plaintiffs failed to allege that the deception occurred in New York, failed to plead their claims with sufficiently particularity to meet the requirements of Rule 9(b), and failed to state their GBL claims based on duties under the FTC Act because it does not provide an ascertainable standard of conduct. These arguments fail.

First, Plaintiffs adequately allege that the deception occurred in New York. Plaintiffs allege that they made Marriott reservations in New York and/or stayed at Marriott properties in New York. Compl. ¶ 936. New York can constitute the place of deception in either scenario, because in both situations Defendants would provide personal information to Marriott and I must grant all inferences in favor of the Plaintiffs. Therefore the Plaintiffs have plausibly alleged the deception occurred in New York.

Second, Plaintiffs' allegations meet the pleading requirements of Rule 9(b). To begin with, the parties dispute whether Rule 9(b)'s pleading requirements apply to the GBL claims. Several federal courts have held that Rule 9(b)'s pleading requirements do not apply to GBL claims. *See, e.g.*, *Pelman ex rel. Pelman v. McDonald's Corp*, 396 F.3d 508, 511 (2d Cir. 2005) ("[B]ecause a private action under § 349 does not require proof of the same essential elements (such as reliance) as common-law fraud, an action under § 349 is not subject to the pleading-with-particularity requirements of Rule 9(b), Fed. R. Civ. P., but need only meet the bare-bones notice-pleading requirements of Rule 8(a), Fed. R. Civ. P"); *Greene v. Gerber Prod. Co.*, 262 F. Supp. 3d 38, 67 (E.D.N.Y. 2017) (same); *Anthem*, 162 F. Supp. 3d at 996–97 (same). Nonetheless, Defendants argue that the Fourth Circuit's pleading rules apply here, and that because the GBL claims sound

in fraud, they must meet the requirements of Rule 9(b). *Cf. Murphy v. Capella Educ. Co*., 589 F. App'x 646, 658 (4th Cir. 2014) (applying Rule 9(b) to Virginia Consumer Protection Act claims); *Jones v. Sears Roebuck & Co*., 301 F. App'x 276, 287 (4th Cir. 2008) (applying Rule 9(b) to West Virginia's Consumer Credit and Protection Act claims); *Lombel*, 2013 WL 5604543, at *6 (applying Rule 9(b) to Maryland Consumer Protection Act claims). I need not decide this issue because for the reasons discussed in Section IV.b above regarding Plaintiffs' Maryland Consumer Protection Act claims, Plaintiffs similar allegations here meet the requirements of either Federal Rule of Civil Procedure 8(a) or 9(b).

Finally, as to Plaintiffs' GBL claims premised on a violation of duties under Section 5 of the FTC Act., for the reasons discussed above in Section II.c regarding the Georgia negligence per claims, Section 5 of the FTC Act provides an ascertainable duty regarding data protection. Moreover, New York courts specifically interpret § 349 "by looking to the definition of deceptive acts and practices under [S]ection 5 of the Federal Trade Commission Act." *New York v. Feldman*, 210 F. Supp. 2d 294, 302 (S.D.N.Y. 2002).

Therefore, Defendants' motion to dismiss the New York GBL claims is denied.

V. Damages

As a final pitch to dismiss all of the Plaintiffs' claims, Defendants argue that Plaintiffs have failed to plead damages. Defendants argue that actual loss is required to plead the negligence and contract claims, and that actual injury is required to plead the statutory claims. Def. Mot. 30–31. But Plaintiffs have pled damages under each of their causes of action. *See* Compl. ¶ 304 (negligence damages), ¶ 311 (negligence per se damages), ¶ 328 (contract damages), ¶ 366 (Maryland PIPA damages), ¶ 381 (Maryland CPA damages), ¶ 457 (California UCL damages), ¶ 784 (Michigan ITPA damages), ¶ 939 (New York GBL damages); *see also* Compl. ¶ 270

(summarizing harms and alleging, "[a]s the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages . . ."). These damages include loss of the benefit-of-the bargain, loss of time and money spent mitigating harms, and loss of value of personal information. *Id.* In addition, some of the Plaintiffs allege losses from identify theft in the form of unauthorized charges and accounts. *See, e.g.*, Compl. ¶¶ 36, 77.

Defendants argue that no Plaintiffs attempt to place a value on the alleged overpayment, loss of benefit-of-the bargain, or loss of value of personal information. Def. Mot. at 31–32. But as explained above, Plaintiffs do not need to assign a value at this stage to adequately plead damages. Defendants also argue that the time and money spent mitigating harms do not qualify as damages because this harm is speculative. This is simply a rehash of Defendants' arguments regarding injury-in-fact. Because I find that the harms here are not speculative, the losses incurred to mitigate the harms are adequately pled damages in addition to being an injury-in-fact. Finally, regarding the fraudulent charges alleged by Plaintiffs Cullen, Golin, and O'Brien, Defendants argue that these plaintiffs do not allege that they were not reimbursed. *Id.* at 32. But that turns the pleading requirement on its head. The pleadings do not indicate that plaintiffs were reimbursed. And at this stage I am required to grant all inferences in favor of Plaintiffs. Therefore, Plaintiffs have adequately alleged actual injury and actual loss to state their contract, negligence, and statutory claims, and Defendants' motion to dismiss on this basis is denied.

Conclusion

In sum, Marriott's motion to dismiss is granted in part and denied in part. Plaintiffs have standing to bring their claims. They have adequately alleged injury-in-fact in the form of losses from identity theft, imminent threat of identity theft, costs spent mitigating the harms from the data

breach, loss of the benefit-of-their-bargain, and loss of value of their personal information. These injuries are fairly traceable to Defendants' conduct. Plaintiffs have also adequately alleged their respective tort, contract, and statutory claims under the laws of California, Florida, Georgia, Maryland, Michigan, New York, and Oregon. These claims may proceed. Plaintiffs' claims for negligence under Illinois law are dismissed. A separate Order follows.

February 21, 2020
Date

/S/
Paul W. Grimm
United States District Judge