UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHANTAL ATTIAS, *et al.*, Plaintiffs, v. **CAREFIRST, INC., *et al.***, Defendants.	Case No. 15-cv-00882 (CRC)

MEMORANDUM OPINION

In May 2015, the District of Columbia-area health insurer CareFirst announced that it had suffered a data breach that compromised the personal information of millions of its policyholders. Plaintiffs in this putative class action are among those whose data was accessed. They seek compensation for the breach through both tort- and contract-based claims under

District of Columbia law, as well as statutory claims under several D.C., Maryland, and Virginia consumer-protection laws.

Common to all of plaintiffs' claims is the assertion that they have been injured by CareFirst's failure to protect their personal information from exposure. The alleged injuries do not, for the most part, involve actual misuse of their personal information. Plaintiffs instead claim that the data breach resulted in an increased *risk* of identity theft and the need for prophylactic expenditures—on credit monitoring services and the like—to reduce that risk. They also contend that CareFirst's failure to protect their personal information resulted in a contractual injury because they did not receive the full value of the policies they purchased. And they say they have suffered emotional distress in dealing with the breach.

The Court previously dismissed plaintiffs' claims for lack of Article III standing, finding that they had failed to allege a non-speculative injury-in-fact. The D.C. Circuit reversed and remanded. CareFirst now moves to dismiss the operative second amended complaint under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim.

The Court will grant the motion in large part. After briefly recounting the factual and procedural background, the Court will begin by confirming that it has diversity jurisdiction over the case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). It will then explain its conclusion that, while plaintiffs' alleged injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the "actual damages" element of nine of their state-law causes of action. The Court will then move to the interplay between plaintiffs' tort and contract claims, finding that the parties' non-fiduciary contractual relationship independently forecloses tort liability based on the allegations in the complaint. Finally, the Court will address issues specific to plaintiffs' unjust enrichment claim and their claims under

the District of Columbia Consumer Protection Procedures Act and the Maryland Consumer Protection Act.

At the end of the day, the Court will dismiss all of plaintiffs' claims except for a breach of contract claim and a Maryland Consumer Protection Act claim brought by the only two plaintiffs (Kurt and Connie Tringler of Maryland) who have plausibly alleged actual misuse of personal information resulting from the data breach. In reaching this outcome, the Court acknowledges the difficulty of applying traditional tort and contract principles in the contemporary context of data security. It also recognizes that courts across the country have divided on a number of important legal issues that frequently arise in data breach litigation. The Court has attempted to illuminate some of these divisions in this opinion.

I. Background

Seven plaintiffs bring this putative class action against CareFirst and certain of its affiliates doing business in the District of Columbia, Maryland, and Virginia. Second Am. Class Action Compl. ("SAC"), ECF No. 9.[1] CareFirst operates a group of health insurance companies providing coverage to more than one million individuals in the District of Columbia, Maryland, and Virginia. Id. ¶¶ 5–8, 23. Plaintiffs are residents of the District of Columbia, Maryland, and Virginia, and customers and insureds of CareFirst. Id. ¶¶ 1–4, 25. When customers purchase health insurance through CareFirst, they provide the company certain personal information, including their names, credit card numbers, addresses, and social security numbers. Id. ¶¶ 26–27. CareFirst promises, explicitly or implicitly, to keep this information protected. Id. ¶¶ 28–29.

[1] The named plaintiffs are Chantal Attias and Andreas Kotzur of the District of Columbia, Richard and Latanya Bailey of Virginia, and Curt and Connie Tringler and Lisa Huber of Maryland. Id. ¶¶ 1–4.

CareFirst allegedly failed to properly encrypt some of the data entrusted to its care, id. ¶ 31, and in June 2014, CareFirst suffered a cyberattack, id. ¶ 33. It learned of the attack in April 2015 and notified its customers, including plaintiffs, the following month. Id. ¶¶ 35–36.

Plaintiffs initiated this action shortly after learning of the data breach and filed the operative second amended complaint in July 2015. They bring eleven claims: breach of contract (Count I), negligence (Count II), violation of the District of Columbia Consumer Protection Procedures Act (Count III), violation of the District of Columbia Data Breach Notification Statute (Count IV), violation of the Maryland Consumer Protection Act (Count V), violation of the Virginia Consumer Protection Act (Count VI), fraud (Count VII), negligence *per se* (Count VIII), unjust enrichment (Count IX), breach of the duty of confidentiality (Count X), and constructive fraud (Count XI). They allege that they "have suffered economic and non-economic loss in the form of mental and emotional pain and suffering and aguish [sic] as a result of Defendants' failures" to secure plaintiffs' confidential information. SAC ¶ 38. The Tringlers specifically allege that they have experienced "tax-refund fraud" as a result of the data breach. Id. ¶ 57. And all plaintiffs allege that they "face years of constant surveillance of their financial and personal records, monitoring, and loss of rights." Id. ¶ 56.

CareFirst moved to dismiss the complaint for lack of subject matter jurisdiction under Rule 12(b)(1) and failure to state a claim under Rule 12(b)(6). The Court granted the 12(b)(1) motion on the ground that plaintiffs had not identified an "actual or imminent" injury as is necessary to satisfy the injury-in-fact requirement of constitutional standing. In so doing, the Court observed that most of the plaintiffs had not alleged that their personal information had actually been misused in any way. Nor had they explained how the information taken (which CareFirst averred did not include financial information or social security numbers) could readily

be used to assume their identities. Based on these factors, the Court adopted the principle that most other courts have followed in similar cases, including a Maryland federal class action brought by another set of CareFirst customers stemming from the same breach: "Absent facts demonstrating a substantial risk that stolen data has been or will be misused in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from wh[ich] the information was taken." Attias v. CareFirst, Inc., 199 F. Supp. 3d 193, 197 (D.D.C. 2016). The Court further held that plaintiffs' other asserted injuries were also insufficient to meet the injury-in-fact requirement of standing. Those harms included (1) expenditures on credit-monitoring services to prevent future identity theft; (2) some indeterminate overpayment for their insurance coverage; (3) loss of the intrinsic value of the stolen personal information; and (4) violation of their statutory rights under various consumer protection laws. Id. at 202–03.

The D.C. Circuit reversed and remanded, finding that plaintiffs had plausibly alleged a substantial risk of identity theft flowing from the data breach, which was enough to meet "the light burden of proof the plaintiffs bear at the pleading stage" of the case. Attias v. CareFirst, Inc., 865 F.3d 620, 627–28 (D.C. Cir. 2017). The Circuit declined to reach CareFirst's alternative argument that plaintiffs had failed to state a claim under Rule 12(b)(6). Id. at 629–30. It did so because this Court had reserved judgment on a second threshold jurisdictional question—whether diversity jurisdiction exists under the Class Action Fairness Act, 28 U.S.C. § 1332(d)—which the Circuit could not answer on the record before it. Attias, 865 F.3d at 629–30.

Venturing once more into the breach, CareFirst has now renewed its 12(b)(6) motion before this Court. Mem. in Supp. of Defs.' Mot. to Dismiss ("MTD"), ECF No. 44-1. Plaintiffs

oppose the motion. Pls.' Opp'n to MTD ("Opp'n"), ECF No. 45. The Court held a hearing on November 5, 2018, and the motion is now ripe for resolution.

II. Standard of Review

In analyzing a motion to dismiss under Rule 12(b)(6), the Court must determine whether the complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). This requires "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. To make this determination, the Court "must take all of the factual allegations in the complaint as true." Id. It also must "construe[] the complaint liberally in the plaintiff's favor with the benefit of all reasonable inferences derived from the facts alleged." Stewart v. Nat'l Educ. Ass'n, 471 F.3d 169, 173 (D.C. Cir. 2006). Finally, the Court may only "consider the facts alleged in the complaint, documents attached thereto or incorporated therein, and matters of which it may take judicial notice." Id.

III. Jurisdiction

The Court turns first to the jurisdictional question that it previously left unresolved: whether it has diversity jurisdiction over plaintiffs' eleven state-law claims under the Class Action Fairness Act ("CAFA"). It does. "CAFA gives federal courts jurisdiction over certain class actions, . . . if the class has more than 100 members, the parties are minimally diverse, and the amount in controversy exceeds $5 million." Dart Cherokee Basin Operating Co., LLC v. Owens, 135 S. Ct. 547, 552 (2014) (citing 28 U.S.C. §§ 1332(d)(2), (5)(B)). Beginning with the first requirement, plaintiffs estimate that there are more than one million class and sub-class members, SAC ¶ 63, and CareFirst does not contest that number for purposes of this motion,

Hr'g Tr. at 3:2–3:14. Second, the parties are minimally diverse because "any member of a class of plaintiffs is a citizen of a State different from any defendant," 28 U.S.C. § 1332(d)(2)(A): The plaintiffs are residents of the District of Columbia, Maryland, and Virginia and have sued CareFirst and its affiliates doing business in those three places. And third, the amount in controversy almost certainly exceeds the $5 million threshold. Under CAFA, the Court aggregates the individual claims of class members. Here, even if individual class members' claims are worth just $5 each, they would satisfy the amount-in-controversy requirement. But it's likely that the value of their claims is much more. For example, plaintiffs have brought claims under the District of Columbia Consumer Protection Procedures Act, D.C. Code Ann. § 28-3901 *et seq.*, which provides statutory damages of $1,500 per violation, and the Virginia Consumer Protection Act ("VCPA"), Va. Code Ann. § 59.1-196 *et seq.*, which entitles successful plaintiffs to $500 to $1,000 per violation. SAC ¶¶ 90(d), 115. Although plaintiffs do not provide a breakdown of the numbers in each subclass, it's hard to imagine a distribution that would not satisfy the amount-in-controversy requirement based solely on these statutory claims. In any event, neither party questions that the amount in controversy exceeds $5 million. See SAC ¶ 10; Hr'g Tr. at 3:2–3:4; Dart Cherokee, 135 S. Ct. at 553 (explaining that amount-in-controversy allegation should be accepted where not questioned by either party).

Accordingly, because the prospective class has more than 100 members, the parties are minimally diverse, and the amount in controversy exceeds $5 million, this Court has diversity jurisdiction under CAFA. See Dart Cherokee, 135 S. Ct. at 552.

IV. Analysis

"A federal court sitting in diversity must apply the substantive law of the jurisdiction in which it sits." Metz v. BAE Sys. Tech. Sol. & Servs. Inc., 774 F.3d 18, 21–22 (D.C. Cir. 2014).

Here, that jurisdiction is the District of Columbia.[2] This means that the Court is bound by decisions of the District of Columbia Court of Appeals—the highest court in D.C.—interpreting D.C. law. Id. This requirement is all the more salient in a data-breach case like this because federal courts across the country have applied the relevant state law to claims arising out of data breaches to very different effect. In the absence of a decision by the District of Columbia Court of Appeals, the Court's role in interpreting and applying D.C. law is to achieve the same outcome it believes would result if the District's highest court considered this case. Id.

As will follow, the Court first concludes that all plaintiffs but the Tringlers have failed to allege, as they must, actual damages for nine of their eleven claims. The Court then finds that plaintiffs' contractual relationship with CareFirst precludes the rest of their claims: their tort claims because they fail to allege an independent duty to safeguard private information; their unjust enrichment claim because they fail to allege that their contract is invalid or unenforceable; and their D.C. Consumer Protection Procedures Act claim because they fail to allege any unlawful trade practice beyond the breach of contract itself. In the end, only the Tringlers remain and they are left only with their breach of contract claim in Count I and their Maryland Consumer Protection Act claim in Count V.

A. Whether plaintiffs have adequately alleged damages for nine of their eleven claims

CareFirst moves to dismiss the following nine of plaintiffs' claims for failure to allege actual damages: (1) breach of contract; (2) negligence and (3) negligence *per se*; (4) fraud and (5) constructive fraud; (6) breach of the duty of confidentiality; violations of the (7) Maryland

[2] Although there was some confusion in the briefing, the parties agreed at the hearing that District of Columbia law applies to all but the state-specific statutory claims. See Opp'n at 12; Hr'g Tr. at 6:2–6:10.

and (8) Virginia Consumer Protection Acts; and violation of the (9) District of Columbia Breach Notification Statute. MTD at 6–10. Plaintiffs counter that CareFirst simply camouflages the "the exact same argument" regarding speculative harm previously rejected by the D.C. Circuit in deciding that they have adequately pled an injury-in-fact for purposes of standing. Opp'n at 1, 5.

The D.C. Circuit's standing ruling does not control whether plaintiffs have alleged actual harm for purposes of their state-law claims. See id. at 6. Plaintiffs may satisfy the Article III injury-in-fact requirement and yet fail to adequately plead damages for a particular cause of action. For example, in Krottner v. Starbucks Corp., 406 F. App'x 129 (9th Cir. 2010), the Ninth Circuit explained that its holding in a concurrently published opinion that the plaintiffs "pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of their state-law claims" arising out of the theft of a company laptop containing the confidential personal information of thousands of Starbucks employees. Id. at 131.[3] The court concluded that, despite having Article III standing based on the risk of future identity theft, the employees failed to state a negligence claim because, under the relevant state law, "[t]he mere danger of future harm, unaccompanied by present damage, will not support a negligence action." Id. (citation omitted). So too here. Although plaintiffs have successfully pled an injury-in-fact sufficient to support federal constitutional standing, they must still plead a proper cause of action under the relevant D.C. or state law.

With that issue aside, the Court now turns to the merits of CareFirst's argument that nine causes of action should be dismissed for failure to plead damages under the applicable state laws.

---

[3] See also Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016) ("As we previously have cautioned, [i]t is crucial . . . not to conflate Article III's requirement of injury in fact with a plaintiff's potential causes of action, for the concepts are not coextensive." (internal quotation marks and citation omitted) (alterations in original)).

1. Plaintiffs must allege actual damages for nine of their causes of action

All but two of plaintiffs' claims require allegations of actual damages.

a. Breach of contract

Under District of Columbia law, actual loss or damage is an essential element for a breach of contract cause of action. See Cahn v. Antioch Univ., 482 A.2d 120, 130 (D.C. 1984) ("It is clear in contract law that a plaintiff is not required to prove the amount of his damages precisely; however, the fact of damage and a reasonable estimate must be established." (quoting W.G. Cornell Co. of Wash., D.C. v. Ceramic Coating Co., Inc., 626 F.2d 990, 993 (D.C. Cir. 1980))); Sloan v. Urban Title Servs., Inc., 689 F. Supp. 2d 123, 133 & 133 n.7 (D.D.C. 2010) ("Both District and Virginia law require proof of injury (*i.e.*, damages) as an element of claims for breach of contract[.]" (citing Osbourne v. Capital City Mortg. Corp., 727 A.2d 322, 324–25 (D.C. 1999))). The mere danger of future harm, unaccompanied by present injury, will not support a breach of contract action. See Sloan, 689 F. Supp. 2d at 134–35.

b. Negligence and negligence *per se*

Under D.C. law, "[t]o maintain an action for negligence, a plaintiff must allege more than speculative harm from defendant's allegedly negligent conduct." Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 708 (D.C. 2009); see also Hillbroom v. PricewaterhouseCoopers LLP, 17 A.3d 566, 573 (D.C. 2011) ("[T]he mere breach of a professional duty, causing only nominal damages, speculative harm, or the threat of future harm—not yet realized—does not suffice to create a cause of action for negligence." (quoting Knight v. Furlow, 553 A.2d 1232, 1235 (D.C. 1989))). The same is true for a negligence *per se* action. See Tolson v. The Hartford Fin. Servs. Grp., Inc., 278 F. Supp. 3d 27, 36 (D.D.C. 2017) (explaining that plaintiff "would still have to prove that she was *injured*" for her negligence *per se* claim).

c. Fraud and constructive fraud

Next, "provable damages" is also an "essential element[] of common law fraud" in the District. Kitt v. Capital Concerts, Inc., 742 A.2d 856, 860–61 (D.C. 1999) (citing Dresser v. Sunderland Apartments Tenants Ass'n, Inc., 465 A.2d 835, 839 (D.C. 1983)); see also Wetzel v. Capital City Real Estate, LLC, 73 A.3d 1000, 1002–03 (D.C. 2013). "Constructive fraud differs from actual fraud only in that the misrepresentation of material fact is not made with the intent to mislead, but is made innocently or negligently." De May v. Moore & Bruce, L.L.P., 584 F. Supp. 2d 170, 185 (D.D.C. 2008) (quoting Nguyen v. Voorthuis Opticians, Inc., 478 F. Supp. 2d 56, 64 (D.D.C. 2007)). As such, constructive fraud also requires actual damages.

d. Breach of the duty of confidentiality

A claim for a breach of the duty of confidentiality is equivalent to a claim for a breach of a fiduciary duty. See Democracy Partners v. Project Veritas Action Fund, 285 F. Supp. 3d 109, 120 (D.D.C. 2018). Under D.C. law, a breach of a fiduciary duty "require[s] a showing of injury or damages." Headfirst Baseball LLC v. Elwood, 239 F. Supp. 3d 7, 14 (D.D.C. 2017); see also Randolph, 973 A.2d at 709.

e. Statutory claims

Under the Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-408(a), a plaintiff must "plead actual injury or harm," Lloyd v. Gen. Motors Corp., 916 A.2d 257, 277 (Md. 2007) (citing Citaramanis v. Hallowell, 613 A.2d 964, 969 (Md. 1992)). "[T]o articulate a cognizable injury under the [Maryland] Consumer Protection Act, the injury must be objectively identifiable," meaning "the consumer must have suffered an identifiable loss, measured by the amount the consumer spent or loss as a result of his or her reliance on the sellers' misrepresentation." Id.

The Virginia Consumer Protection Act also requires a plaintiff to plead actual loss in order to bring a suit for damages under the Act. See Polk v. Crown Auto, Inc., 228 F.3d 541, 543 (4th Cir. 2000) (citing Va. Code Ann. § 59.1-204(A)); see also Chisholm v. TranSouth Fin. Corp., 194 F.R.D. 538, 549 (E.D. Va. 2000).

Finally, by its terms, the District of Columbia Data Breach Notification Act likewise requires "actual damages," which do "not include dignitary damages, including pain and suffering." D.C. Code Ann. § 28-3853(a).

2. Four theories of actual damages

The Court discerns four possible theories of actual damages in plaintiffs' complaint and briefing: (1) actual and/or heightened risk of misuse of personal information, (2) loss of the "benefit of the bargain" they struck when they purchased their policies, (3) consequential damages like expenditures credit monitoring services, and (4) emotional distress. The Court will address each theory in turn.

a. Misuse of personal information

The first theory of damages may be the most obvious in the context of a data breach: actual or heightened risk of misuse of exposed personal information. Plaintiffs generally allege that they have suffered both an "increased risk of identity theft, and also actual identity theft and resulting losses." SAC ¶ 17. They continue, "[m]any Plaintiffs and Class Members suffered from actual economic injury resulting in tax-refund fraud, identity theft, credit card fraud, and other conduct causing direct economic injury as a result of the identity theft they suffered." Id. ¶ 20; see also id. ¶ 58 ("many Plaintiffs have already suffered from direct economic injury such as tax-refund fraud, identity theft, [and] credit card fraud.").

The rub, though, is that only two of the named plaintiffs—the Tringlers from Maryland—actually allege that they have already experienced any kind of economic injury. The Trinlgers contend that they "*have* experienced tax-refund fraud" as a result of the breach. Id. ¶ 57 (emphasis added).[4] The rest claim only the threat of misuse by listing what "identity thieves" "*can*" or "*may*" do with the kind of personal information accessed. See id. ¶¶ 49–51, 55 (emphases added). But the District of Columbia Court of Appeals has expressly declined to treat an increased risk of future identity theft as an actual harm for purposes of negligence and breach of fiduciary duty claims based on data breaches. See Randolph, 973 A.2d at 708–09.[5] And there is no reason to believe that court would decide any differently if presented with plaintiffs' other causes of action that require actual harm.

Plaintiffs do not confront the substance of this binding decision of the District of Columbia Court of Appeals head on. Instead, they incorrectly describe Randolph as a case about "the law of standing." Opp'n at 10 n.4. Although the lower court did conclude that the Randolph plaintiffs lacked standing, the D.C. Court of Appeals clearly explained that "the better approach toward resolving [the] motion to dismiss is to analyze whether the amended complaint succeeded in stating a claim." Randolph, 973 A.2d at 707.

---

[4] While the Tringlers have not alleged specific facts connecting the two events, the Court must draw all reasonable inferences in favor of plaintiffs when considering a motion under Rule 12(b)(6). Accordingly, even though the Tringlers may ultimately fail to prove causation at summary judgment, it can be plausibly inferred for present purposes.

[5] Randolph is not an outlier. Other courts across the country have likewise distinguished between plaintiffs whose data has been exposed *and* misused and those whose data has been exposed but not misused for purposes of claims requiring actual damages. See, e.g., Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.").

Accordingly, with respect to plaintiffs' negligence and breach of fiduciary duty claims, the Court is bound by the Randolph decision. And, because this Court sitting in diversity is charged with determining how the D.C. Court of Appeals would rule in the absence of a case directly on point, the Court concludes that the D.C. Court of Appeals would likely hold, consistent with Randolph, that the mere threat of misuse of personal information would not be sufficient to state a claim for actual damages under the remaining seven claims not addressed in that decision. Thus, under District of Columbia law, only the Tringlers have alleged actual damages under this first theory of damages—misuse of exposed personal information.

b. Benefit of the bargain theory of damages

Plaintiffs also contend that they were harmed by "a loss of the benefit of the bargain." Opp'n at 5–6. Under this theory, plaintiffs allege that they "provided payment to Defendants for certain services, including health insurance coverage, part of which was intended to pay administrative costs of securing their [sensitive personal information]." SAC ¶ 25. In return, however, they "received services devoid of these very important protections." Id. ¶ 26. In other words, plaintiffs allege that they overpaid for their health insurance because they contracted for a service that would include data security but received a service that did not. This "benefit of the bargain" loss is, plaintiffs say, "the standard measure" of damages in breach of contract claims. Opp'n at 8.

District of Columbia courts have not addressed whether a "benefit-of-the-bargain" or "overpayment" theory of damages is sufficient to state a claim for actual damages in the data-breach context. But two fellow courts in this district have addressed the theory when considering 12(b)(1) motions to dismiss for lack of standing, and both rejected it as too "indeterminate." In In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litigation, 45 F. Supp. 3d 14 (D.D.C.

2014) ("SAIC"), for example, Judge Boasberg rejected the data-breach plaintiffs' argument that they plausibly alleged "actual loss" by "claim[ing] that some indeterminate part of their premiums went toward paying for security measures." Id. at 30. He explained that the plaintiffs had not alleged that the money paid could have gone towards a better data-security policy or "that the market value of their insurance coverage (plus security services) was somehow less than what they paid." Id.; see also Austin-Spearman v. AARP & AARP Servs. Inc., 119 F. Supp. 3d 1, 13–14 (D.D.C. 2015) (K.B. Jackson, J.) (concluding that plaintiff failed to plausibly plead economic injury-in-fact based on an "overpayment" theory—that is, that she paid for an online membership that included particular data-security benefits but received one that did not (citing SAIC, 45 F. Supp. 3d at 30)).[6]

As is often the case in the data-breach context, there are courts that disagree. The Eighth Circuit, for example, has held that a plaintiff plausibly alleged an injury-in-fact for standing based on a "devaluation" of his video-game 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." Carlsen, 833 F.3d at 909. And Judge Koh in the Northern District of California has generally embraced the benefit-of-the-

[6] Courts in other jurisdictions have likewise concluded that alleged overpayment for health insurance that does not include bargained-for data security is not sufficient to allege injury-in-fact for purposes of standing. See Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 754–55 (W.D.N.Y. 2017) (listing cases). In Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564 (D. Md. 2016), the Maryland class action arising out of the same CareFirst data breach, the court rejected the plaintiffs' benefit-of-the-bargain theory of injury in finding a lack of standing. The court explained, "Plaintiffs make no allegations that the data breach diminished the value of the health insurance they purchased from CareFirst" nor do they offer "factual allegations indicating that the prices they paid for health insurance included a sum to be used for data security." Id. at 572. As a result, the Chambliss plaintiffs did not "quantify this alleged loss." Id. So too here.

bargain theory when considering 12(b)(6) motions in data-breach cases. See In re Yahoo! Inc. Customer Data Sec. Breach Litig., 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018) (concluding that plaintiff's "allegations are sufficient to allege that he suffered benefit-of-the-bargain losses" because he "pleads that he has paid $19.95 each year since December 2007 for Yahoo's premium email service," which was supposed to be "secure," and he would not have signed up "had he known that Yahoo's email service was not as secure as [Yahoo] represented"); In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 992, 995 (N.D. Cal. 2016) (adopting "loss of benefit of the bargain" theory of "actual harm" for New York plaintiffs who alleged they had contracted for "reasonable and adequate security measures" that Anthem failed to deliver, causing plaintiffs to overpay for their health insurance); In re Anthem, Inc. Data Breach Litig., No. 15-md-2617, 2016 WL 3029783, at *12–13 (N.D. Cal. May 27, 2016) (concluding same for California plaintiffs' breach-of-contract claim, which required "appreciable and actual" damages).

At the hearing, plaintiffs argued that "there has been a definite trend" away from the conclusion in cases like SAIC and towards those in cases like Anthem and Yahoo!. Hr'g Tr. at 35:2–35:6. But trend or no across the country, the Court declines to go beyond the decisions of its fellow courts in cases like SAIC and Austin-Spearman in the absence of controlling law from the District of Columbia Court of Appeals, especially because the standard for alleging actual damages is generally higher than that for plausibly alleging an injury-in-fact. Moreover, as in SAIC, plaintiffs here broadly allege that some indeterminate amount of their health insurance premiums went towards providing data security. SAC ¶ 25. And as in SAIC, they allege only in conclusory fashion that the services they received "were of a diminished value." Id. ¶ 73. This distinguishes the allegations here from those in In re Yahoo!, for example, where the plaintiffs

put a number—the $19.95 subscription fee for a premium email service with allegedly better security—on the value of the contracted-for data security. Accordingly, the Court concludes that plaintiffs fail to state a claim for actual damages under their benefit-of-the-bargain theory.

c. "Mitigation costs" theory of damages

Plaintiffs devote much of their opposition brief to a third theory of damages, this one related to their efforts to protect against identity theft. They allege that they "have or will have to spend significant time and money to protect themselves." SAC ¶ 19. These costs include "the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, cost of conducting a damage assessment, mitigation costs, costs to rehabilitate [their sensitive information], and costs to reimburse from losses incurred as a proximate result of the breach." Id. It is unclear whether plaintiffs contend that this category of "mitigation" costs constitutes economic damage in its own right or is recoverable as consequential damages. Compare SAC ¶ 17 (Plaintiffs "need to take immediate action to protect themselves from identity theft, which have already and will continue to result in real and actual loss regardless of whether identity theft actually occurs."); Opp'n at 5 (describing "the loss of money and time in the form of expenditures made to protect themselves" as "actual economic damage"); Hr'g Tr. at 45:17 (describing "loss mitigation" as "direct economic harm"), with Opp'n at 7 ("Plaintiffs have alleged that as a consequence of Defendants' failures, breaches and misrepresentations, they have lost time and money."); id. at 8 ("[P]laintiffs who allege a breach of contract may recover both consequential and incidental damages.").

The District of Columbia Court of Appeals has rejected the theory that prophylactic mitigation measures constitute actual damages in their own right. In Randolph, the court explained that no plaintiff had alleged any misuse of any personal information that had been

compromised by the theft of a company laptop containing personal information. 973 A.2d at 708. The court then addressed the plaintiffs' alternative argument regarding preventative expenditures:

> [T]o the extent [the plaintiffs] allege actual harm from expenses they have incurred to undertake credit monitoring or other security measures to guard against possible misuse of their data, they have alleged an injury that is 'not the result of any present injury, but rather the [result of] the anticipation of future injury that has not materialized.'

973 A.2d at 708 (citation omitted) (third alteration in original). Because "the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury the law [of negligence] is prepared to remedy," id. (alteration in original) (quoting Shafran v. Harley-Davidson, No. 07-cv-1365, 2008 WL 763177, at *3 (S.D.N.Y. Mar. 24, 2008)), the court concluded that the plaintiffs had failed to state a negligence claim. The court dismissed the plaintiffs' common-law breach of fiduciary duty claim "[f]or much the same reason." Id. at 709.[7] Under Randolph, then, time and money spent protecting against future identity theft cannot constitute damage in their own right for purposes of plaintiffs' negligence and breach of fiduciary duty claims.[8] And again, there is no reason to believe the D.C. Court of Appeals would treat plaintiffs' other D.C. law claims any differently.

---

[7] Cf. In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1, 40 (D.D.C. 2017), appeal filed No. 18-1182 (dismissing case for lack of subject matter jurisdiction where plaintiffs failed to allege facts that would support waiver of sovereign immunity under Privacy Act because "those plaintiffs who purchased credit monitoring services or incurred other expenses to prevent future identity theft have not suffered actual damages because expenditures undertaken voluntarily to prevent possible future harm do not constitute actual damages" (citation omitted)).

[8] The D.C. Circuit concluded that plaintiffs plausibly alleged redressability for purposes of Article III standing because they "reasonably spent money to protect themselves against a substantial risk," meaning they could "be made whole by monetary damages." Attias, 865 F.3d at 629. But again, Article III standing and actual damages are separate questions governed by

This is consistent with how the vast majority of courts have treated mitigation costs in the context of data-breach litigation. They have distinguished between plaintiffs whose information has been exposed *and* misused and those whose information has been exposed but not misused. These courts draw the line at responsive versus preventative expenditures. For the former, costs are generally recoverable as consequential damages; for the latter, costs are not actual damages in their own right and cannot be recovered as consequential damages because there is not an actual injury, only an anticipated one.

For example, in Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007), the Seventh Circuit considered whether Indiana contract and tort law would permit recovery for the cost of "past and future credit monitoring services" incurred by bank customers after a hacker accessed their confidential information on the bank's website. Id. at 631, 635. "Significantly, the plaintiffs did not allege any *completed direct* financial loss to their accounts . . . . [n]or did they claim that they . . . *already had been* the victim of identity theft[.]" Id. at 632. The court concluded that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy" by expending time and resources to monitor and protect their identities. Id. at 639; see also, e.g., Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (rejecting "plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss," which would have been "a novel legal theory of damages" for a breach of contract in Michigan, "based on a risk of injury at some indefinite time in the future"); Forbes v. Wells

---

federal and state law respectively. Therefore, the preventative measures plaintiffs have taken may be sufficient to support redressability but are not, under D.C. law, sufficient as actual damages.

Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006) (rejecting plaintiffs' contention for both negligence and breach-of-contract claims "that the time and money they have spent monitoring their credit suffices to establish damages" in "anticipation of future injury that has not materialized").

Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018), on which plaintiffs rely, see Opp'n at 7, is not to the contrary. In that case, a class of plaintiffs sued Barnes & Noble after discovering that hackers had accessed individuals' names and credit card information on the company's computer system. Dieffenbach, 887 F.3d at 827. A named plaintiff from California alleged four kinds of injury stemming from the data breach after someone used her account "to make a fraudulent purchase": a delay in the restoration of funds to her bank account, the time she spent coordinating with the police and her bank, a delay in her ability to use the compromised account, and her failure to receive the full measure of her bargain with Barnes & Noble. Id. at 828–29. The Seventh Circuit concluded that the first three losses were actual economic injuries sufficient to state a claim. Id. at 829.[9] The same was true for the named plaintiff from Illinois, who decided to renew her monthly credit-monitoring service after her bank contacted her about a potentially fraudulent charge and froze her card for several days. Id. In other words, the Seventh Circuit considered credit-monitoring and other mitigation services to be cognizable injuries for both named plaintiffs *who alleged they were already experiencing actual misuse*. See also Anthem, 2016 WL 3029783, at *15–16 (describing these kind of mitigation costs as

[9] Hewing to the result in the majority of cases cited in Section (IV)(A)(2)(b) above, the Seventh Circuit rejected the argument that the plaintiff suffered an economic "benefit of the bargain" loss because she did not contend that any of the items she purchased were "defective" or that "Barnes & Noble promised any particular level of security, for which she paid." Id. at 829.

"consequential out of pocket expenses" where plaintiff was notified his personal information was stolen, he learned that his financial information had been "compromised" and "used for unauthorized charges," and *then* he "took actions to prevent further financial damage").

Apart from the Tringlers, plaintiffs here complain only of the cost of prophylactic, rather than responsive, measures. Consistent with the weight of authority on this issue, the remaining plaintiffs who have not alleged actual misuse of their exposed personal information may not plead actual damages under a mitigation-cost theory. Only the Tringlers—who, as discussed above, have alleged actual misuse in the form of tax-refund fraud—would be able to recover consequential damages like the money spent monitoring their credit.

d. Emotional distress

Finally, plaintiffs seek non-economic damages for five of the nine claims that require actual damage: negligence, SAC ¶ 83; negligence *per se*, id. ¶ 129; violation of the Maryland Consumer Protection Act ("MCPA"), id. ¶ 109; fraud, id. ¶ 122; and constructive fraud, id. ¶ 152.[10] They claim that, in addition to economic loss, they have suffered "non-economic loss in the form of mental and emotional pain and suffering and aguish [sic] as a result of Defendants' failures." Id. ¶ 38. Based on the Court's conclusions regarding plaintiffs' theories of economic loss, all but the Tringlers are left with allegations of purely emotional damages. At the hearing, CareFirst took the position that emotional distress alone may as a matter of law sustain a claim

[10] Plaintiffs do not seek emotional distress damages for their breach of contract, D.C. Data Breach Notification Statute, Virginia Consumer Protection Act, and breach of the duty of confidentiality claims. Id. ¶¶ 74, 97, 114, 144. In any event, emotional distress damages would not be recoverable for at least some of these claims. See Howard Univ. v. Baten, 632 A.2d 389, 392 (D.C. 1993) (breach of contract); D.C. Code ¶ 28-3853(a) (excluding "dignitary harms, including pain and suffering," from the definition of "[a]ctual damages" under the D.C. Data Breach Notification Statute).

for actual damages, but that here, plaintiffs have failed to adequately plead emotional distress. Hr'g Tr. at 15:24–16:15. The Court sees two questions: first, whether a plaintiff may sustain a claim for negligence, fraud, or violation of the MCPA based solely on emotional distress; and second, whether plaintiffs have adequately pled such damages here.

The District of Columbia Court of Appeals applies "a different framework" for "[c]laims of negligence that seek damages for only mental pain and suffering." Hedgepeth v. Whitman Walker Clinic, 22 A.3d 789, 795 (D.C. 2011). To state a claim where "emotional distress is the only injury suffered," id. at 810, the plaintiff must satisfy either the "zone of physical danger" rule set out in Williams v. Baker, 572 A.2d 1062 (D.C. 1990) (en banc), or the special relationship and undertaking rule set out in Hedgepeth, 22 A.3d at 810–11. Such "negligent infliction of emotional distress" claims are distinct from other negligence claims where the plaintiff seeks to recover for pain and suffering as "parasitic" damages as a result of or incident to the "invasion of another legally protected interest." Hedgepeth, 22 A.3d at 809.

Plaintiffs' allegations regarding their pain and suffering are too conclusory to satisfy either the Williams or Hedgepeth rule. See Hawkins v. Wash. Metro. Area Transit Auth., 311 F. Supp. 3d 94, 107–08 (D.D.C. 2018) (dismissing negligent infliction of emotional distress claim where plaintiffs failed to plead "serious and verifiable" emotional distress). This makes sense: Plaintiffs did not set out to state a claim only for emotional damages. Rather, they seek "ancillary or 'parasitic' damages for related mental distress (sometimes referred to as 'pain and suffering')." Hedgepeth, 22 A.3d at 795. As such, they cannot sustain their negligence and negligence *per se* claims based on emotional distress alone.

The same is true for plaintiffs' fraud and constructive fraud claims. Although a plaintiff may seek both economic and emotional damages in an action for intentional fraud, Osbourne v.

Capital City Mort. Corp., 667 A.2d 1321, 1328 (D.C. 1995), superseded by statute on other grounds, D.C. Code Ann. § 28-3905(k)(1), the "*sine qua non* of any recovery for misrepresentation is a showing of pecuniary loss proximately caused by reliance on the misrepresentation," Kitt, 742 A.2d at 861 (quoting Day v. Avery, 548 F.2d 1018, 1029 (D.C. Cir. 1976) (per curiam)). Put another way, the economic torts of fraud and constructive fraud require some showing of economic harm in order for the plaintiff to recover emotional damages as well.

And finally, the Maryland Court of Appeals has held that the MCPA permits "recovery of damages for emotional distress if there [is] at least a 'consequential' physical injury,'" but not where the plaintiff makes allegations like, "This made me feel bad; this upset me." Sager v. Hous. Comm'n of Anne Arundel Cty., 855 F. Supp. 2d 524, 548–49 (D.D.C. 2012) (quoting Hoffman v. Stamper, 867 A.2d 276, 296 (Md. 2005)). Plaintiffs' allegations are more akin to the latter than the former, and thus cannot support a claim for a violation of the MCPA based on emotional distress alone.

Accordingly, plaintiffs' allegations of emotional distress are not sufficient to sustain their claims for negligence or negligence *per se*, fraud or constructive fraud, or violation of the MCPA.

* * *

Based on the foregoing, the Court will dismiss the following claims: breach of contract, negligence, negligence *per se*, fraud, constructive fraud, and breach of the duty of confidentiality brought by all plaintiffs but the Tringlers. The Court will also dismiss the District of Columbia Breach Notification Statute claim brought on behalf of the D.C. plaintiffs and the Virginia Consumer Protection Act claim brought on behalf of the Virginia plaintiffs. Finally, the Court will dismiss the Maryland Consumer Protection Act claim brought by Ms. Huber but not by the

Tringlers. This leaves (at this point) the Tringlers with all of their claims; the D.C. plaintiffs with their unjust enrichment and D.C. Consumer Protection Procedures Act claims; the Virginia plaintiffs with their unjust enrichment claim; and Ms. Huber with her unjust enrichment claim. The Court now moves to the interplay between plaintiffs' contract and tort claims.

B. Whether the parties' contractual relationship bars plaintiffs' tort claims

As an alternative to its arguments that plaintiffs fail to plead damages, CareFirst moves to dismiss plaintiffs' five tort claims—negligence, negligence *per se*, fraud, constructive fraud, and breach of aduty of confidentiality—based on the parties' contractual relationship. CareFirst asserts that plaintiffs cannot recover in tort for breach of duties that merely restate CareFirst's alleged contractual duties. According to CareFirst, because plaintiffs have failed to allege an independent common-law duty to reasonably safeguard personal information separate from any contractual one, they cannot "double dip" with claims sounding in tort. And even if there is such a duty, CareFirst asserts that the "economic loss rule" bars recovery here because, in the absence of a "special relationship" between parties, plaintiffs may not recover purely economic loses in tort. Finally, CareFirst contends that insurers and insureds do not have a fiduciary relationship that would support plaintiffs' claim for breach of a duty of confidentiality.

The Court starts and stops with the independent duty rule. Because the Court concludes that plaintiffs have failed to allege a duty to reasonably safeguard insureds' data separate from CareFirst's contractual duties—in part because the parties do not have a fiduciary relationship—it need not reach whether the parties are in a special relationship such that the economic loss rule would not apply.

"The failure to perform a contractual obligation typically does not give rise to a cause of action in tort." Jones v. Hartford Life & Accident Ins. Co., 443 F. Supp. 2d 3, 5 (D.D.C. 2006).

Under D.C. law, for a plaintiff to recover in tort for conduct that also constitutes a breach of contract, "the tort must exist in its own right independent of the contract, and any duty upon which the tort is based must flow from considerations other than the contractual relationship." Choharis v. State Farm Fire & Cas. Co., 961 A.2d 1080, 1089 (D.C. 2008). Thus, the viability of plaintiffs' tort claims turns on whether plaintiffs have plausibly alleged that CareFirst owes them an independent duty of care to reasonably safeguard private information beyond the parties' contractual relationship.

They have not. The complaint alleges no "facts separable from the terms of the contract upon which the tort may independently rest" and identifies no "duty independent of that arising out of the contract itself." Id. Plaintiffs assert that they "contracted for services that included a promise by Defendants to safeguard, protect, and not disclosure [sic] their personal information . . . ." SAC ¶ 26; id. ¶ 66. They identify four sources of this promise: two CareFirst privacy policies, id. ¶¶ 28, 29, 67; its written services contract, which "promised" that CareFirst would "only disclose health information when required to do so by federal or state law," id. ¶ 66; and its "promise[] to comply with all HIPAA standards," id. ¶ 68. Plaintiffs' breach-of-contract claim turns on CareFirst's alleged breach of these promises. Id. ¶¶ 34, 72. Plaintiffs' negligence claim does not include additional facts or identify a separate duty to safeguard personal data; instead, it simply alleges that CareFirst "owed the Plaintiffs a duty of care in protecting the confidentiality of the personal and private information that the Plaintiffs provided to the Defendants as consumers of the Defendants' health insurance policies." Id. ¶ 77. This allegation makes clear that "the duty of which [plaintiffs] essentially complain[]"—the duty to reasonably safeguard insureds' personal information—"necessarily arose from the contractual relationship." Nugent v. Unum Life Ins. Co. of Am., 752 F. Supp. 2d 46, 54 (D.D.C. 2010). But for the

contract between CareFirst and plaintiffs, CareFirst would not have had access to plaintiffs' information and thus would have had no occasion—or obligation—to protect it.[11]

Plaintiffs' response to Choharis is two-fold and doubly unsuccessful. First, they misinterpret its holding as being limited to a particular kind of tort—a first-party bad faith cause of action. See Opp'n at 17. The Choharis court clearly applied the broad rule—that "the tort must exist in its own right independent of the contract"—beyond the tort of bad faith to fraud and negligent misrepresentation as well. 961 A.2d at 1089–90 (affirming summary judgment where plaintiff's "assertions [regarding "fraudulent or negligent misrepresentation"] directly related to an obligation arising under the contract"). Plaintiffs' second argument implicitly reveals the error of their narrow interpretation of the case by attempting to fit their allegations into the Choharis framework: They contend that they have in fact alleged an "independent injury over and above the mere disappointment of plaintiff's hope to receive his contracted-for-benefit" because they do not allege that any "health insurance benefits were wrongfully denied." Opp'n at 17–18 (quoting Choharis, 961 A.2d at 1089). Put differently, they attempt—for purposes of their tort claims—to limit the contract's reach to the mere provision of health insurance benefits. But that argument undermines their contractual one—namely, that they "contracted for services

---

[11] Other federal courts across the country have dismissed data-breach negligence claims where the plaintiffs failed to identify a non-contractual duty to safeguard private information. See, e.g., Gordon v. Chipotle Mexican Grill, Inc., No. 17-cv-1415-CMA-MLC, 2018 WL 3653173, at *16–17 (D. Colo. Aug. 1, 2018), magistrate R&R adopted in relevant part by 2018 WL 4620342, at *10 (D. Colo. Sept. 26, 2018) (dismissing negligence claim in consumer data breach case where "[p]laintiffs do not cite any Colorado authorities to support [the assertion that] Defendant had an independent duty to safeguard [private information]" and plaintiffs "alleged the same duty under their implied contract"); SELCO Cmty. Credit Union v. Noodles & Co., 267 F. Supp. 3d 1288, 1295 (D. Colo. 2017) (dismissing financial-institution data breach case where plaintiffs "cite no support for the existence of specific common law or statutory duties of care related to data security" and "most important of all," the duties alleged by plaintiffs were "created by, and completely contained in, the contractual provisions" (citation omitted)).

that included a guarantee by Defendant to safeguard their personal information." SAC ¶ 21. Plaintiffs cannot have their cake (a contract that sets forth specific promises to safeguard information) and eat it too (a contract that provides only for the provision of health insurance).[12] Plaintiffs therefore fail to satisfy the Choharis requirement that they allege a tort duty independent of CareFirst's contractual obligations.[13]

---

[12] Plaintiffs advanced a version of this argument at the hearing. When asked to explain where in the complaint they allege an independent duty, counsel responded that CareFirst's "privacy policy" constitutes "a separate representation" from the contractual representations that more obviously relate to health insurance, like a promise to "cover my claim if I hurt my leg." Hr'g Tr. at 42:11–42:18. But when the Court pointed out that plaintiffs also base their contract claim in part on the promises made in those policies, counsel simply responded, "[i]t's broken promises in the four corners of the contract, and it's broken promises outside of the four corners of the contract." Id. at 44:20–44:22. This response only reinforces the Court's conclusion that plaintiffs have not alleged an *independent* duty.

[13] Responding to CareFirst's arguments regarding the economic loss rule, plaintiffs contend that "it has already been held that an insurer has 'additional obligations' beyond those stated in a contract by nature of the insurer-insured relationship." Opp'n at 15 (citing Cent. Armature Works, Inc. v. Am. Motorists Ins. Co., 520 F. Supp. 283, 292 (D.D.C. 1980)). Although it does not reach the economic loss rule arguments, the Court will address this contention to the extent it can be construed as asserting that such "additional obligations" give rise to some sort of independent duty. In Central Armature Works, the court upheld an award of punitive damages in a breach of contract action against an insurance company in part because "an insurer has additional obligations to its insured which subject it to more stringent standards of conduct than those normally imposed on parties to a contract." 520 F. Supp. at 292. Acknowledging that "[n]either party [] presented any authority from the District of Columbia which establishes the relationship between an insurer and its insured," id., the court relied on out-of-district precedent and a general assertion by the District of Columbia Court of Appeals that insurers have a "duty to process and pay claims expeditiously and in good faith," id. (quoting Cont'l Ins. Co. v. Lynham, 293 A.2d 481, 483 (D.C. 1972)). In 1993, the D.C. Circuit likewise relied on out-of-district precedent to explain that the "bad faith tort [for "refusal to pay insurance benefits"] is grounded on the covenant of good faith and fair dealing that is implicit in all contracts [and] supplemented by the idea that insurance contracts have special characteristics that warrant heightened liability for breach of that covenant." Messina v. Nationwide Mut. Ins. Co., 998 F.2d 2, 5 (D.C. Cir. 1993). But since Central Armature Works and Messina, "the D.C. Court of Appeals has spoken clearly and 'bad faith conduct,' to the extent proved, 'can be compensated within those principles' of the contractual obligation of good faith and fair dealing." Nugent, 752 F. Supp. 2d at 56 (quoting Choharis, 961 A.2d at 1087). Coming full circle, then, plaintiffs'

Even where plaintiffs fail to identify a non-contractual duty, some courts outside this jurisdiction have recognized a stand-alone duty to provide reasonable data security separate from any operative agreement. The District of Columbia Court of Appeals has not confronted this question. And jurisdictions across the country are divided as to whether there is a common law duty to provide data security. The courts that have recognized such a duty have rooted it in one, or a combination, of three theories: an affirmative duty to refrain from causing others harm, the foreseeability of harm, or the nature of the parties' relationship. The Court considers these theories in turn.

First, some courts have recognized a duty to provide reasonable data security under the "basic principle" of tort law that "everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm." In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (quoting Yakubowicz v. Paramount Pictures Corp., 536 N.E.2d 1067, 1070 (Mass. 1989)). The Sony court concluded that this general duty to *refrain* translated to a specific "legal duty to *provide* reasonable network security . . . separate and independent from the PSN User Agreement" and any contractual obligations that arose from that agreement. Id. at 968 (emphasis added). Because Sony allegedly breached that duty by "fail[ing] to employ reasonable security measures to protect" the plaintiffs' personal information—"provided . . . to Sony as part of a commercial transaction"—

---

overreading of Central Armature Works to impose a separate *tort* as opposed to *contractual* obligation is foreclosed by Choharis.

the plaintiffs could "pursue both contract and tort remedies, to the extent [their] tort claims are not barred by the economic loss doctrine." Id.[14]

The Court is not persuaded by Sony's reasoning because it elides the distinction between a duty to refrain and a duty to act. While there may be a general duty to refrain from acts that cause others harm, this usually does not extend to an obligation to act affirmatively. Here, as in Sony, plaintiffs allege that CareFirst *failed* to act by not employing reasonable security measures to protect customers' personal information. The Court hesitates to recognize a common-law duty based on that alleged omission. See also Veridian Credit Union v. Eddie Bauer, LLC, 295 F. Supp. 3d 1140, 1158 (W.D. Wash. 2017) (finding no common law duty to reasonably secure credit card information where plaintiffs' "allegations comprise numerous omissions or nonfeasance on the part of Eddie Bauer, but they do not describe misfeasance or any affirmative act 'that created a situation of peril' for [plaintiffs]" (citation omitted)).

Still, there are some circumstances under District of Columbia law where even a failure to act will give rise to a legal duty. "[W]hether a duty exists is the result of a variety of considerations." Bd. of Tr. of Univ. of Dist. of Columbia v. DiSalvo, 974 A.2d 868, 871 (D.C. 2009). These considerations include the foreseeability of harm and the nature of the relationship between the parties. Id. at 871–72 & 871 n.2; see also Hedgepeth, 22 A.3d at 794 ("We have described a court's examination of whether a duty exists as a 'foreseeability of harm test' that is determined, in large part, by the nature of the relationship between the parties." (quoting Odemns

[14] Demonstrating the complicated interaction between the independent duty doctrine and the economic loss rule, the Sony court ultimately concluded that the "special relationship" exception to the economic loss rule did not apply because the plaintiffs "failed to allege a 'special relationship' with Sony beyond those envisioned in everyday consumer transactions." Id. at 969. "[T]herefore, negligence [was] the wrong legal theory on which to pursue recovery for [their] economic losses." Id.

v. District of Columbia, 930 A.2d 137, 143 (D.C. 2007)). The balance of these considerations operates on "a sliding scale: If the relationship between the parties strongly suggests a duty of protection, then specific evidence of foreseeability is less important, whereas if the relationship is not of a type that entails a duty of protection, then the evidentiary hurdle is higher." DiSalvo, 974 A.2d at 872 (quoting Workman v. United Methodist Comm. on Relief, 320 F.3d 259, 264 (D.C. Cir. 2003)).

This leads to the second theory: Some of the courts that have recognized a common law duty to reasonably secure consumers' data have done so based on the foreseeability of harm. For example, in In re Arby's Restaurant Group, Inc. Litigation, No. 1:17-cv-514-AT, 2018 WL 2128441 (N.D. Ga. Mar. 5, 2018), a group of financial institutions and consumers sued Arby's after hackers breached the restaurant's point of sales machines. Id. at *1. Applying Georgia law, the court emphasized the role that "foreseeability" plays "in defining the existence of a legal duty." Id. at *3. More specifically, the Arby's court explained that under state law, a person or entity "may still have a duty to protect against a criminal act of a third person," which would include hacking into a private data system, "if it is alleged that [the entity] had 'reason to anticipate' the criminal act." Id. (citation omitted). In that case, the plaintiffs alleged that Arby's knew or should have known about the risk of a data breach based on known problems specific to Arby's point of sales system as well as other recent highly publicized data breaches in that industry. Id. at *5. The court found those allegations "sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss." Id.; id. at *12 (concluding that both tort and contract actions could proceed because plaintiffs identified "a common law duty that would

have applied regardless of the existence of an underlying contract").[15] Here, by contrast, plaintiffs have made no allegations that it was foreseeable that CareFirst specifically would suffer a data breach based on, for instance, known vulnerabilities in its data-storage systems.

And third, some courts that have recognized a common law duty in the data-breach context have done so based on the nature of the relationship between the party providing the confidential information and the party receiving it, as well as the sensitive nature of the information provided. An inquiry into the nature of the relationship often overlaps with two separate but related legal questions: whether the "special relationship" exception to the economic loss rule barring tort claims applies and whether there is a fiduciary relationship to support a duty of confidentiality. In some cases, the analysis merges entirely.

Take Daly v. Metropolitan Life Insurance Co., 782 N.Y.S. 2d 530 (N.Y. Sup. Ct. 2004), where a New York trial court considered "a new area of law"—namely, "whether liability may attach to an entity that fails to safeguard personal and confidential information obtained in conjunction with the purchase of a life insurance policy." Id. at 532. In the absence of case law on this then-nascent legal question, the court drew a parallel to the breach of a fiduciary duty of confidentiality, where one party puts its trust in the other by relying on the other's superior expertise. Id. at 534–35. The court analogized that the insurance company—like a fiduciary—"had a duty to protect the confidential personal information provided by" subscribers because

---

[15] See also, e.g., In re The Home Depot, Inc. Customer Data Sec. Breach Litig., No. 1:14-md-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."); In re Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1310 (D. Minn. 2014) (same).

insurance subscribers were "required to" provide the insurance company "with highly sensitive personal information" in order to obtain life insurance and that company had represented in its privacy notice that it would safeguard that information. Id. at 535. At least one federal district court has adopted Daly's reasoning. In Jones v. Commerce Bancorp, Inc., the court concluded that a bank customer sufficiently alleged a legal duty to safeguard information where the bank required her to provide confidential personal information in order to open a business account and warranted that it would safeguard that information. No. 06-cv-835-HB, 2006 WL 1409492, at *1–2 (S.D.N.Y. May 23, 2006) (citing Daly, 782 N.Y.S. 2d 532–35).

The problems of data breaches may no longer be "new" but courts around the country continue to confront these legal questions. Just recently, for example, the Pennsylvania Supreme Court held for the first time that "an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system." Dittman v. UPMC, 196 A.3d 1036, 1038 (Pa. 2018). The court rooted this duty in the traditional common law duty to exercise reasonable care when engaging in affirmative conduct as well as the nature of the relationship between the parties. The employees alleged that "as a condition of their employment," their employer "required them to provide certain personal and financial information, which [it] collected and stored on its internet-accessible computer system without use of adequate security measures." Id. at 1047. According to the court, this dynamic was sufficient to allege a duty of care. Id.

Not all courts, however, have concluded that requiring another to provide sensitive personal information creates such a duty. For example, in Cooney v. Chicago Public Schools, 943 N.E.2d 23 (Ill. App. Ct. 2010), the Appellate Court of Illinois concluded that Chicago Public Schools did not owe a legal duty to safeguard its employees' personal information. Id. at 29. In

that case, the Chicago Board of Education inadvertently disclosed the personal information, including social security numbers and health insurance plan information, of almost 2,000 former employees. Id. at 27. The employees urged the court to "recognize a 'new common law duty' to safeguard information" in light of the sensitive nature of personal data that was disclosed and the fact that the Board had collected that data. Id. at 28–29. But the Illinois court declined to go beyond state statutory notice requirements and recognize a new duty in the absence of specific authority. Id. at 29. "Federal courts interpreting Illinois law have consistently declined to impose a common law duty to safeguard personal information in data security cases" based on Cooney. In re SuperValu, Inc., Customer Data Sec. Breach Litig., 14-md-2586-ADM-TNL, 2018 WL 1189327, *14 (D. Minn. Mar. 7, 2018). In SuperValu, for instance, consumers argued that SuperValu owed them "an extra-contractual duty" because it "solicited customers' [private personal information] and thus had a duty to take reasonable measures to safeguard their data and notify them of any data breach." Id. The district court declined to recognize such a duty. Id.; see also, e.g., Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 816 (7th Cir. 2018) (relying on Cooney to conclude that Illinois "would not impose the common law data security duty the plaintiff banks call for here"); Gordon, 2018 WL 3653173, at *15 (citing Cooney and Community Bank of Trenton to dismiss an Illinois negligence claim "for lack of a common law duty").

Because the District of Columbia Court of Appeals has not determined one way or the other whether there is a common law duty to safeguard data, the Court will follow the approach taken in some of the cases cited above and look to analogous case law regarding the nature of the relationship between insurers and insureds. "District of Columbia law does not . . . consider the relationship between insurer and insured a fiduciary relationship" as a matter of law.

Gebretsadike v. Travelers Home & Marine Ins. Co., 103 F. Supp. 3d 78, 83 (D.D.C. 2015) (citing Fireman's Fund Ins. Co. v. CTIA-The Wireless Ass'n, 480 F. Supp. 2d 7, 15 (D.D.C. 2007)); see also Stevens v. United Gen. Title Ins. Co., 801 A.2d 61, 66 (D.C. 2002) (applying contract rather than fiduciary principles to determine whether duty to defend exists). This is consistent with other jurisdictions. Instead, the relationship between parties to an insurance contract is generally considered "contractual in nature." See Fero, 236 F. Supp. 3d at 773-74 (quoting Batas v. Prudential Ins. Co. of Am., 281 A.D. 2d 260, 264 (N.Y. Sup. Ct. 2001)) (declining to recognize a "special relationship" necessary for negligent misrepresentation claim between health insurance provider and consumers whose confidential health information was accessed), withdrawn on other grounds by 304 F. Supp. 3d 333 (W.D.N.Y. 2018); In re Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1203 (D. Or. 2016) ("[T]he nature of the relationship between the parties [consumers and their insurance company] is not the type of relationship that historically has been considered fiduciary in character."); Dolmage v. Combined Ins. Co. of Am., No. 14-cv-3809, 2015 WL 292947, at *6 (N.D. Ill. Jan. 21, 2015) ("In Illinois, it is well settled that no fiduciary relationship exists between an insurer and an insured as a matter of law." (internal alterations, quotation marks, citation omitted)).

Plaintiffs try to avoid this precedent by reframing their relationship with CareFirst as a doctor-patient one, which has been historically recognized as a fiduciary relationship as a matter of law. See Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 591–92 (D.C. 1985). They allege—for purposes of their breach of the duty of confidentiality claim *only*—that CareFirst owed them such a duty "pursuant to its fiduciary relationship with the Plaintiffs . . . as their *health care providers*." SAC ¶ 139 (emphasis added). But CareFist obviously is not a provider of healthcare; it is a provider of health care *insurance*, as plaintiffs repeatedly acknowledge

elsewhere throughout their complaint. See, e.g., SAC ¶ 23 ("Defendants are a network of for-profit *health insurers* which provide *health insurance coverage* to individuals[.] (emphases added)); see also id. ¶¶ 25, 60, 65, 77, 89, 125. Accordingly, no doctor-patient relationship exists that would give rise to a duty of confidentiality as a matter of law.

Even where, as here, a fiduciary relationship does not exist as a matter of law, District of Columbia courts may imply such a relationship in special circumstances. Determining whether a fiduciary relationship exists requires "a searching inquiry into the nature of the relationship, the promises made, the types of services or advice given and the legitimate expectations of the parties." Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz, 793 F. Supp. 2d 311, 341 (D.D.C. 2011) (quoting Firestone v. Firestone, 76 F.3d 1205, 1211 (D.C. Cir. 1996)); Church of Scientology Int'l v. Eli Lilly & Co., 848 F. Supp. 1018, 1028 (D.D.C. 1994) (recognizing that even though "no Court has ever found there to be a fiduciary relationship between a public relations firm and one of its clients," the court faced a "fact-intensive question" about "the nature of the relationship" specific to the parties before it). In addition, "a fiduciary relationship could exist [] where circumstances show that the parties extended their relationship beyond the limits of the contractual obligations to a relationship founded upon trust and confidence." Paul v. Judicial Watch, Inc., 543 F. Supp. 2d 1, 6 (D.D.C. 2008) (citing Church of Scientology, 848 F. Supp. at 1028); see also Ying Qing Lu v. Lezell, 919 F. Supp. 2d 1, 6 (D.D.C. 2013) ("While fiduciary relationships can be difficult to define, and may very well exist between contracting parties, '[o]ne characteristic that District of Columbia courts have traditionally looked for is a "special confidential relationship" that transcends an ordinary business transaction and requires each party to act with the interests of the other in mind.'" (citing High v. McLean Fin. Corp., 659 F. Supp. 1561, 1568 (D.D.C. 1987))).

Plaintiffs fail to plead anything to suggest that their relationship with CareFirst was anything more than the typical commercial relationship between insurer and insureds. As in Fero, nothing about the alleged "interactions would appear to fall outside the scope of what is routine between insurers and insureds, and therefore, the interactions do no suggest any kind of special relationship of trust and confidence." 236 F. Supp. 3d at 773–74. True, CareFirst required plaintiffs to provide personal and confidential information, but this will be the case in almost every insurer-insured relationship. Plaintiffs do not allege a relationship beyond that envisioned in every day interactions with a health insurance provider that would give rise to either a common law duty to safeguard private information or a fiduciary duty. As such, negligence, negligence *per se*, and breach of the duty of confidentiality are misplaced legal theories on which to pursue recovery for the data breach.

The same is true for plaintiffs' fraud and constructive fraud claims, which likewise arise out of the same alleged conduct that supports their breach of contract claim. "District of Columbia law requires that the factual basis for a fraud claim be separate from any breach of contract claim that may be asserted." Plesha v. Ferguson, 725 F. Supp. 2d 106, 113 (D.D.C. 2010) (citing Choharis, 961 A.2d at 1089). The plaintiffs in Plesha failed to satisfy this requirement because their allegations of fraud arose out of the same alleged conduct by defendants—"late payments and promises to pay"—that provided the basis for their breach of contract claim. Id. So too here. For their contract claim, plaintiffs allege that CareFirst breached its "promise[] through its Internet Privacy Policy that it would encrypt all personal information given to Defendants." SAC ¶¶ 67, 72. For their fraud claim, plaintiffs similarly allege that CareFirst "made false representations of material facts" in its "Internet Privacy Policy and General Privacy Policy, which indicated that information provided . . . would be encrypted."

Id. ¶ 118; see also id. ¶ 150 (alleging, for constructive fraud claim, that CareFirst owed plaintiffs a duty "to abide by the privacy policies it had incorporated and to safeguard personal health information"). CareFirst's allegedly unfulfilled promise to encrypt all personal information thus cannot constitute a separately actionable fraud or constructive fraud claim.

* * *

Based on the foregoing, the Court will dismiss all plaintiffs' tort claims, including negligence, negligence *per se*, breach of the duty of confidentiality, fraud, and constructive fraud. This leaves the following: the Tringlers with their breach of contract, unjust enrichment, and Maryland Consumer Protection Act claims; Ms. Huber of Maryland with her unjust enrichment claim; the D.C. plaintiffs with their unjust enrichment and D.C. Consumer Protection Procedures Act claims; and the Virginia plaintiffs with their unjust enrichment claim. The Court turns next to unjust enrichment.

C. Whether plaintiffs have pled in the alternative an unjust enrichment claim

CareFirst contends that its undisputed contractual relationship with plaintiffs also precludes their unjust enrichment claim. MTD at 15–16. It is well-established that the existence of a valid contract precludes a claim for unjust enrichment. See, e.g., Harrington v. Trotman, 983 A.2d 342, 346 (D.C. 2009) (holding that superior court "fundamentally erred as a matter of law in finding unjust enrichment when there was a valid contract between the parties"). Plaintiffs counter that while they cannot ultimately recover under both theories, they may plead unjust enrichment in the alternative should the Court later find no contractual agreement between the parties. Opp'n at 18–19. True enough, courts "sometimes permit[] a party to plead [unjust enrichment] as an alternative in certain circumstances." He Depu v. Yahoo! Inc., 306 F. Supp. 3d 181, 193–94 (D.D.C. 2018) (citation omitted). But the devil is in the details: Such an

alternative theory "require[s] an allegation that the contract is invalid and unenforceable." Id. Plaintiffs have not alleged this, and CareFirst confirmed at the hearing that it has not taken the position that the contract is invalid or unenforceable. See Sony, 996 F. Supp. 2d at 984–85, 984 n.37 (dismissing unjust enrichment claims, pled in the alternative, where plaintiffs did not challenge validity or enforceability of user agreements); Hr'g Tr. 20:5–20:11.

Accordingly, the Court will dismiss the unjust enrichment claim for all plaintiffs. This leaves unaddressed the D.C. Consumer Protection Procedures Act claim brought on behalf of the D.C. plaintiffs and the Maryland Consumer Protection Act claim brought on behalf of the Tringlers.[16]

D. Whether plaintiffs have alleged an unlawful trade practice under the D.C. Consumer Protection Procedures Act

Like their tort claims, the District of Columbia plaintiffs' D.C. Consumer Protection Procedures Act ("DCCPPA") claim is premised on CareFirst's alleged breach of its contractual obligations. They allege that CareFirst "violated [its] Internet Privacy Policy" and thus "committed and [sic] unfair and unlawful trade practice" by not providing the benefits provided for in that policy and misrepresenting a material fact "as indicated in their Internet Privacy Policy." SAC ¶ 88.[17]

---

[16] Remember that the Court dismissed the MCPA claim brought on behalf of the other Maryland plaintiff, Ms. Huber, because she failed to allege actual damages.

[17] Plaintiffs also alleged that CareFirst violated the DCCPPA by failing to comply with HIPAA. Originally, CareFirst moved to dismiss the DCCPPA claim (as well as the breach of contract, negligence, and negligence *per se* claims) as premised on an alleged violation of HIPAA, which does not have a private right of action. MTD at 16. Plaintiffs have since disavowed reliance on alleged HIPAA violations for all but their negligence *per se* claim. Opp'n at 19. Because the Court has already concluded that plaintiffs have not stated a claim for negligence *per se* due to their failure to allege actual damages and their failure to identify an independent duty, it need not address this alternative basis for dismissal.

The Court can interpret plaintiffs' DCCPPA allegations in one of two ways, neither of which passes muster. On the one hand, plaintiffs could be alleging that the mere breach of contract constitutes an unlawful trade practice under the DCCPPA. But they cite no support for this proposition and at least one court in this district has implied that a DCCPPA claim must be premised on at least *some* additional conduct other than a run-of-the-mill breach. See Jacobson v. Hofgard, 168 F. Supp. 3d 187, 199–200, 206–07 (D.D.C. 2016) (denying motion to dismiss because DCCPPA claim was not "inappropriately duplicative of Plaintiffs' breach of contract claim" where alleged misrepresentation preceded the formation of the contract); see also Am. Airlines, Inc. v. Wolens, 513 U.S. 219, 233 (1995) (concluding, under Illinois law, that "a breach of contract, without more, 'does not amount to a cause of action cognizable under the Consumer Fraud Act and the Act should not apply to simply breach of contract claims" (internal alterations, quotation marks, citation omitted)).

On the other hand, plaintiffs could be alleging that CareFirst "misrepresented a material fact"—which would constitute an unlawful trade practice under the DCCPPA—by stating that it would comply with the terms of its Internet Privacy Policy knowing full well that it would not. But another court in this district has concluded that under D.C. law, "an intentional breach of contract"—which is essentially what plaintiffs would need to argue under this misrepresentation theory—"is not punishable as an unlawful trade practice under the Consumer Protection Procedures Act simply because the breach was intended when the contract was formed." Slinski v. Bank of Am., N.A., 981 F. Supp. 2d 19, 36 (D.D.C. 2013). The Court agrees with that reasoning.

Accordingly, because the D.C. plaintiffs' DCCPPA claim is entirely duplicative of their breach of contract claim and an intentional breach of contract cannot constitute an unlawful trade practice, the Court will dismiss this claim as well.

E. Whether insurance companies are exempt from civil liability for data breaches under the Maryland Consumer Protection Act

Last but not least, the Court addresses CareFirst's argument that all of the plaintiffs' claims under the Maryland Consumer Protection Act ("MCPA")—including the Tringlers'—must be dismissed because the Act exempts insurance companies from liability. MTD at 19–20. The MCPA expressly states that its provisions do not apply to the "professional services" of an "insurance company." Md. Code Ann., Com. Law § 13-104(1). The question then is whether "professional services" as that term is used under the Act applies to the data-security services at issue in this case.

Maryland's highest court has interpreted "professional services" narrowly as applied to "medical or dental practitioner[s]," who are also exempt under the MCPA. In Scull v. Groover, Christie & Merritt, P.C., 76 A.3d 1186 (Md. 2013), the Maryland Court of Appeals held that a radiology office's medical-billing practices were not exempt under the professional-services exemption because those practices were related to the "commercial or entrepreneurial" aspects of the office rather than the "actual rendering of health care services." Id. at 1196, 1197–98.[18] To reach this conclusion, the court considered the statutory function of the state's Consumer

[18] CareFirst relies on outdated case law to argue that the professional-services exemption applies "broadly" even when one acts outside their professional capacity. MTD at 20 (citing Lembach v. Bierman, 528 F. App'x 297, 304 (4th Cir. 2013)). For this proposition, the Fourth Circuit in Lembach relied on the Maryland Court of Special Appeals' decision in Scull v. Doctors Groover, Christie & Merritt, P.C., 45 A.3d 925 (Md. Ct. Spec. App. 2012). But the Fourth Circuit issued Lembach in June 2013, before Maryland's highest court reversed in relevant part the Court of Special Appeals' decision below. See Scull, 76 A.3d at 1196–97.

Protection Division's ("CPD") Health Education and Advocacy Unit, which is authorized to refer disputes regarding a medical provider's billing practices, but not the adequacy of its treatment, to the CPD for potential enforcement actions, as well as the CPD's longstanding view that the MCPA applies to medical-billing practices. Id. at 1194–95. The court also considered the legislative history of another exemption directed specifically at health care services. Id. at 1194. Finally, the court identified other areas of the law that distinguish between the ancillary services of a medical office like billing and the more direct services like treating a wound or implanting a dental filling. For example, professionals are generally licensed based on specialized training and expertise directly related to their profession. Id. at 1195–96. And for negligence actions, a professional is generally held to a special standard of care applicable to their particular profession. Id.

The Court concludes that the professional-services exemption of the MCPA does not apply to CareFirst's data-security practices. Rather, gathering and storing consumers' private information is ancillary to the provision of health insurance coverage much like billing is ancillary to the provision of medical care. Other areas of Maryland law reinforce the conclusion that an insurance company's data-security practices are not exempt as a professional service. Maryland's Personal Information Protection Act provides that "a business that owns or licenses personal information of an individual" must "implement and maintain reasonable security procedures and practices" in order to "protect personal information from unauthorized access, use, modification, or disclosure." Md. Code Ann., Com. Law § 14-3503. Under the Act, "business" is defined broadly to include any "business entity," and "personal information" is defined broadly to include data like a person's name combined with their social security number, credit card number, or health information. Id. § 14-3501(b)(1) & (e)(1). Health information is in

turn defined as "any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996" ("HIPAA"). Id. § 14-3501(d). As a health insurance provider covered by HIPAA, CareFirst appears to be subject to the Personal Information Protection Act. And because consumers may bring a violation of that Act as an unfair or deceptive trade practice under the MCPA, id. § 14-3508, exempting CareFirst's data-security services from the MCPA would create an inconsistency in state law similar to the one the Scull court tried to avoid.

Therefore, the Court will deny CareFirst's motion to dismiss the Tringlers' Maryland Consumer Protection Act claim.

V. Conclusion

For the foregoing reasons, Defendants' motion to dismiss will be granted in part and denied in part. The Court will grant the motion to dismiss for all but the Tringlers' breach of contract claim in Count I and the Maryland Consumer Protection Act claim in Count V. A separate order accompanies this memorandum opinion.

Christopher R. Cooper

CHRISTOPHER R. COOPER
United States District Judge

Date: January 30, 2019