IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)	MDL No. 1:19md2915 (AJT/JFA)
This Document Relates to CONSUMER Cases	)	

ORDER

Defendants Capital One and Amazon have filed Motions to Dismiss the Amended Corrected Representative Complaint. [Doc. 386] ("Capital One Motion"); [Doc. 394] ("Amazon Motion") (the "Motions").[1] For the reasons stated herein, the Motions are **GRANTED** in part and **DENIED** in part as follows:

1. As to Count 1 (negligence), the negligence claims under the laws of Washington are dismissed; and the Motions are otherwise denied;
2. As to Count 2 (negligence *per se*), the negligence *per se* claims under the laws of California, Florida, Texas, Virginia, and Washington are dismissed; and the Motions are otherwise denied;
3. As to Count 3 (unjust enrichment), the Motions are denied;
4. As to Count 4 (declaratory judgment), the Motions are denied;
5. As to Count 5 (breach of confidence), the breach of confidence claims under the laws of California, New York, Texas, Virginia, and Washington are dismissed; and the Motions are otherwise denied;
6. As to Count 6 (breach of contract), the Capital One Motion is denied;

[1] Unless indicated otherwise, all docket references are made to 1:19-md-2915.

7. As to Count 7 (breach of implied contract), the Capital One Motion is denied;
8. As to Count 8 (California Unfair Competition Law), the Motions are denied;
9. As to Count 9 (California Consumer Legal Remedies Act), the Motions are denied;
10. As to Count 10 (Florida Deceptive and Unfair Trade Practices Act), the claim against Capital One is dismissed as abandoned; and the Motions are otherwise denied;
11. As to Count 11 (New York General Business Law (Count 11), the Motions are denied;
12. As to Count 12 (Texas Deceptive Trade Practices Act—Consumer Protection Act (Count 12), the Motions are denied;
13. As to Count 13 (Virginia Personal Information Breach Notification Act), the Motions are denied;
14. As to Count 14 (Washington Data Breach Notification Act), the Motions are denied; and
15. As to Count 15 (Washington Consumer Protection Act), the Motions are denied.

I. BACKGROUND

The following facts are alleged in Plaintiff's Amended Corrected Representative Consumer Class Action Complaint [Doc. 826] ("Amended Complaint" or "Am. Compl."), which are accepted as true for purposes of this Order.[2] *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007).

On July 29, 2019, Capital One announced it had experienced a data breach of Capital One's Amazon Web Services ("AWS") cloud environment where Capital One was storing

[2] On September 7, 2020, Plaintiff, without objection from Defendants, filed the Amended Complaint, in which the only change was the substitution of the Texas Plaintiff. At the September 8, 2020 monthly status conference, the Court ordered that the Amended Complaint shall be deemed filed and served as the operative complaint; and that the then-pending Motions would be deemed filed and ruled on with respect to the Amended Complaint.

consumers' confidential personal information ("PII") (the "Data Breach"). The Data Breach was the result of a well-known vulnerability of the AWS cloud to an SSRF attack. *See id.* ¶¶ 2, 46-61. Over 100 million people in the United States and six million people in Canada were affected. Am. Compl. ¶¶ 1, 62. Amazon has described the Data Breach through this alleged SSRF breach as follows:

> As Capital One outlined in their public announcement, the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended. After gaining access through the misconfigured firewall and having broader permission to access resources, we believe a SSRF attack was used (which is one of several ways an attacker could have potentially gotten access to data once they got in through the misconfigured firewall).

Id. ¶ 70.

Despite the sophisticated nature of the hack, *id.* ¶ 72, Defendants were well-aware of the AWS cloud's vulnerabilities to unauthorized access through a SSRF attack, *Id.* ¶¶ 46-49. Nevertheless, Capital One chose to place and aggregate its most sensitive consumer information on these susceptible servers and behind AWS's flawed firewall, *Id.* ¶¶ 44, 47-50, and in an attempt to protect against this vulnerability, Capital One and Amazon jointly developed a product called Cloud Custodian, whose purpose was to address the SSRF threat by encrypting data on the AWS servers. *Id.* ¶¶ 56-58. But these efforts were inadequate to secure Capital One customers' data. *Id.* ¶ 58. Indeed, if an unauthorized individual were able to gain access to a credential in the AWS cloud environment, known technically as an "Identity Access Management" role, the credential would allow the unauthorized individual broad access beyond the firewall protecting the cloud and automatic decryption of the data stored in the cloud. *Id.* ¶¶ 47-54, 58-61. In other words, once in the AWS server environment, any individual could access, in Capital One's internal servers an aggregated collection of customers' PII (a data lake), the

precise vulnerability exploited to exfiltrate Capital One's customer data in the Data Breach. *See id*. ¶¶ 65-73.

The Data Breach's occurrence is well documented. Capital One's logs showed a hacker's connections or attempted connections to the AWS server in March and April 2019. However, it was not until July 17, 2019, approximately four months after the Data Breach, that Capital One received an e-mail through its responsible disclosure program raising the possibility that someone had stolen data stored in Capital One's AWS cloud environment. *Id*. ¶¶ 64-65. Shortly thereafter, the person accused of perpetrating the attack, former AWS systems engineer Paige Thompson, was arrested and indicted in federal court. As alleged in the criminal complaint, Thompson gained unauthorized access to Capital One's AWS environment primarily by exploiting a Web Application Firewall ("WAF") that monitored traffic to and from Capital One's AWS cloud environment. *Id*. ¶¶ 65, 67. By exploiting the WAF, Thompson was able to retrieve, access, and exfiltrate data from a portion of the AWS Simple Storage Service buckets in Capital One's AWS environment. *Id*. ¶ 67. Thompson ultimately stole approximately 1.75 terabytes of data on March 22-23, 2019. In addition to the access on March 22, 2019 and 23, 2019, Thompson had also scanned, probed, or accessed Capital One's network on five (5) further instances over a three-month period: March 4, March 12, April 2, April 19, and May 26, 2019. *Id*. ¶ 74. And as further detailed in the criminal complaint, on April 21, 2019, Thompson publicly posted on Github instructions on how she carried out the SSRF attack. *Id*.[3] Thompson then posted openly on Twitter and on public Slack channels over the course of several months

[3] Following Thompson's arrest on July 29, 2019, law enforcement authorities appear to have recovered Capital One's stolen data from Thompson's devices and learned that she was maintaining the stolen data in an encrypted format. *See United States v. Paige A. Thompson, a/k/a "erratic,"* Criminal Compl. ¶¶ 20, 27, No. 2:19-cr-00159-RSL (W.D. Wash. July 29, 2019). The criminal complaint filed alleges that Thompson "intended to disseminate data stolen from victim entities, starting with Capital One." *Id*. ¶ 25.

that she found huge files of data intended to be secured on various AWS cloud servers—including the cloud server for Capital One. *Id*. ¶¶ 78-82.

Plaintiffs seek to represent a putative nationwide class of all individuals whose personal information was compromised in the Data Breach, *id*. ¶ 146, as well as statewide subclasses of affected individuals in California, Florida, New York, Texas, Virginia, and Washington, *id*. ¶ 148. Plaintiffs allege that, as a result of the Data Breach, they suffered various harms including mitigation efforts or expenses (such as time and money spent placing credit freezes on their accounts, setting up credit alerts, and purchasing credit monitoring), diminution in the value of their personal information, and increased risk of future identity theft or other fraud. *See* Am. Compl. ¶¶ 18-27, 142. Plaintiffs also allege they "did not receive the benefit of their bargain" because, had they known the "truth" about Capital One's "data security practices," they would not have applied for Capital One credit cards or been willing to pay as much as they did for Capital One's services. *Id*. ¶ 145. Finally, a subset of seven Plaintiffs—plaintiffs Behar, Gershen, Palencia, Spacek, Sharp, Tada, and Zielicke—allege that they "experienced identity theft and fraud," *id*. ¶¶ 20, 21, 23, 27, or have identified unauthorized activity on their accounts, such as unauthorized charges or attempts to open new accounts after the Data Breach, *id*. ¶¶ 19, 24, 26.

In its Amended Complaint, Plaintiffs asserts the following seven (7) causes of action on behalf of a putative nationwide class of all persons whose PII was compromised in the Data Breach: (1) negligence (Count 1); (2) negligence *per se* (Count 2); (3) unjust enrichment (Count 3); (4) declaratory judgment (Count 4);[4] (5) breach of confidence (Count 5); (6) breach of

[4] Capital One has not moved to dismiss Plaintiffs' claims for declaratory and injunctive relief pertaining to Capital One's allegedly inadequate data security measures. As discussed *infra*, Amazon has moved to dismiss Plaintiffs' claim of declaratory and injunctive relief.

implied contract (Count 6); and (7) breach of contract (Count 7).[5] Am. Compl. ¶¶ 160-229. The Amended Complaint also asserts claims under California, Florida,[6] New York, Texas, and Washington consumer protection statutes and Virginia and Washington data breach notification statutes (Counts 8- 15). *Id*. ¶¶ 230-310.

II. LEGAL STANDARD

A Rule 12(b)(6) motion to dismiss tests the legal sufficiency of the complaint. *See Randall v. United States*, 30 F.3d 518, 522 (4th Cir. 1994); *Republican Party of N.C. v. Martin*, 980 F.2d 943, 952 (4th Cir. 1994). A claim should be dismissed "if, after accepting all well-pleaded allegations in the plaintiff's complaint as true . . . it appears certain that the plaintiff cannot prove any set of facts in support of his claim entitling him to relief." *Edwards v. City of Goldsboro*, 178 F.3d 231, 244 (4th Cir. 1999); *see also Trulock v. Freeh*, 275 F.3d 391, 405 (4th Cir. 2001). In considering a motion to dismiss, "the material allegations of the complaint are taken as admitted," *Jenkins v. McKeithen*, 395 U.S. 411, 421 (1969) (citations omitted), and the court may consider exhibits attached to the complaint, *Fayetteville Investors v. Commercial Builders, Inc.*, 936 F. 2d 1462, 1465 (4th Cir. 1991). Moreover, "the complaint is to be liberally construed in favor of plaintiff." *Id.*; *see also Bd. of Trustees v. Sullivant Ave. Properties, LLC*, 508 F. Supp. 2d 473, 475 (E.D. Va. 2007).

In addition, a motion to dismiss must be assessed in light of Rule 8's liberal pleading standards, which require only "a short and plain statement of the claim showing that the pleader

[5] Counts 5 (breach of confidence), 6 (breach of implied contract), and 7 (breach of contract) are not alleged against Amazon.

[6] Plaintiffs have since abandoned the Florida consumer protection claim as to Capital One. *See* [Doc. 427] at n.27 ("Plaintiffs do not dispute that they do not state a claim against Capital One for violation of the Florida Deceptive and Unfair Trade Practices Act."). Plaintiffs, however, continue to assert this claim against Amazon.

is entitled to relief." Fed. R. Civ. P. 8. Nevertheless, while Rule 8 does not require "detailed factual allegations," a plaintiff must still prov*id*e "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (the complaint "must be enough to raise a right to relief above the speculative level" to one that is "plausible on its face"); *see also Giarratano v. Johnson*, 521 F.3d 298, 302 (4th Cir. 2008). As the Supreme Court stated in *Ashcroft v. Iqbal*, "[a] claim has facial plausibility when the plaintiff pleads factual content that allows the Court to draw a reasonable inference that the defendant is liable for the conduct alleged." 556 U.S. 662, 678 (2008).

III. ANALYSIS

A. Choice of Law

As an initial matter, the Court must consider what law applies when considering the Motions. *See Mothershead v. Xede Consulting Grp., Inc.*, No. 1:14-cv-1205 (AJT/MSN), 2015 WL 12591801, at *2 (E.D. Va. Mar. 30, 2015); *Pa. Emp., Benefit Trust Fund v. Zeneca, Inc.*, 710 F. Supp. 2d 458, 466 (D. Del. 2010) (before addressing a motion to dismiss, "the Court must first resolve the choice of law question to determine the applicable law relevant to each [claim]"). Based on the language in the Cardholder Agreements, Compl. ¶¶ 18-27, Capital One contends that Virginia law (and only Virginia law) applies to Plaintiffs' claims. Plaintiffs contend that at this stage the Court cannot decide what law governs any particular claim since the Cardholder Agreement is not sufficiently alleged in the Complaint to be considered, [Doc. 427] at 7-8, and, in any event, selecting the governing law is a fact-intensive exercise that requires a more extensive record.

The Complaint alleges that each named plaintiff is (or was) a Capital One customer, Am. Compl. ¶¶ 16-17, and no Plaintiff would have used a Capital One credit card "on the applicable terms" (*i.e.*, the terms in the Cardholder Agreements) had they known about Capital One's allegedly deficient data security, *id*. ¶ 1. These allegations sufficiently reference the contractual arrangement that accompanied the credit card services from Capital One that are central to Plaintiffs' claims and the Cardholder Agreements are therefore "integral" to those allegations for the Court to consider them for purposes of the Motions. *See Philips v. Pitt Cty. Mem'l Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009) (explaining that at the motion to dismiss stage, courts may consider documents attached to a motion to dismiss "so long as they are integral to the complaint and authentic"); *Blankenship v. Manchin*, 471 F.3d 523, 526 n.1 (4th Cir. 2006) (noting consideration of matters attached to defendant's motion to dismiss that are integral to complaint). However, for the reasons discussed below, the Court cannot decide within the context of the pending Motions whether Virginia substantive law must apply to each of Plaintiffs' claims under Virginia's choice of law rules.

The Cardholder Agreement includes a section entitled "The Law That Applies to Your Agreement," which states:

> We make decisions to grant credit and issue you a Card from our offices in Virginia. This Agreement is *governed by* applicable federal law and *by Virginia law*. If any part of this Agreement is unenforceable, the remaining parts will remain in effect.

[Doc. 387], Ex. 2 ("Cardholder Agreement") at 5 (emphasis added).[7] A federal court exercising diversity jurisdiction must apply the choice of law rules of the forum state—in this case, Virginia. *See Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496-97 (1941). Virginia law

[7] Capital One has provided the Cardholder Agreement for each of the representative Plaintiffs, except for Plaintiff Palencia, who replaced Plaintiff Muhammed after briefing on the Motions closed. *See* [Doc. 387], Exs. 3-10.

looks favorably upon choice-of-law clauses in a contract, giving them full effect except in unusual circumstances. *See Hitachi Credit Am. Corp. v. Signet Bank,* 166 F.3d 614, 624 (4th Cir 1999) (citing *Tate v. Hain*, 181 Va. 402, 25 S.E.2d 321, 324 (Va. 1943)). The Cardholder Agreement unambiguously refers to Virginia law; and there are no unique circumstances not to apply the clause's choice-of-law provision.

There is no dispute that Plaintiffs' breach of contract claim (raised solely against Capital One) is governed by Virginia law. Capital One, citing the choice-of-law provision in the Cardholder Agreement, contends, however, that Virginia substantive law must apply to *all* claims raised in the Amended Complaint, including its tort claims that would otherwise be subject to foreign law under Virginia's choice-of-law rules. *See* [Doc. 387] at 10 (citing *Run Them Sweet, LLC v. CPA Global Ltd.*, 224 F. Supp. 3d 462 (E.D. Va. 2016) (Ellis, J.)).

Contracting parties express their intention "in the words they have used," and as such, courts must examine those words to ascertain the parties' intent. *W.F. Magann Corp. v. Virginia-Carolina Elec. Works, Inc.*, 203 Va. 259, 264, 123 S.E.2d 377 (Va. 1962). Here, the Court must give effect to the words used (and not used) in the Cardholder Agreement. The Cardholder Agreement unambiguously states that "*this [Cardholder] Agreement* is governed by …Virginia law" (emphasis added). There is no language in the Cardholder Agreement that can be reasonably construed to exclude the application of Virginia's choice of law rules, which are part and parcel of that governing Virginia law. Indeed, Capital One's position ignores the general rule that, when reference is made to a state's substantive law, that reference includes, in the absence of any statement otherwise, the referenced state's choice-of-law rules. *See ITCO Corp. v. Michelin Tire Corp., Commercial Div.*, 722 F.2d 42, 49 n.11 (4th Cir. 1983) (finding that, notwithstanding contract's choice-of-law provision that directs the application of New York

law, because the nature of the liability is *ex delicto*, not *ex contractu*, the relevant state law (North Carolina) would apply); *see also United Dominion Indus. v. Overhead Door Corp.*, 762 F. Supp. 126, 128 (W.D.N.C. 1991) ("The contractual provision here may govern the choice-of-laws as to the interpretation and construction of the contract; however, it does not provide the applicable law for a claim based on unfair and deceptive acts."); *cf. Freedman v. Am. Online, Inc.*, 325 F. Supp. 2d 638, 653 (E.D. Va. 2004) ("[B]ecause the Member Agreement's choice-of-law provision states that 'the laws of the Commonwealth of Virginia, excluding the conflicts-of-law rules, govern this Agreement and your membership,' Virginia substantive law, and not Virginia choice-of-law, applies here . . ." and noting that the authority makes clear that a "choice-of-law provision, like any other contractual provision, must not be applied more broadly than the parties' intended"). As discussed below, whether there are cognizable tort claims will depend in large part of the applicability of the economic loss rule under the laws of the various jurisdictions; but whether those claims exist will be determined by the applicable law under Virginia's choice-of-law rules, not Virginia substantive law.[8]

[8] The Court recognizes the tension between this decision and *Run Them Sweet.* In *Run Them Sweet*, this Court concluded that all claims, including non-contractual claims, were to be governed by Virginia law, without regard to Virginia's choice of law rules, based on the following choice of law and forum selection clause:

> These conditions and any contract made under them shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, United States of America, with the understanding that any legal action taken regarding this Agreement shall be brought in a U.S. District Court located in the Commonwealth of Virginia.

Run Them Sweet, 224 F. Supp. 3d at 464. The choice-of-law clause here is substantively different than the clause at issue in *Run Them Sweet.* Here, the relevant provision does not contain a forum selection provision and is entitled "The Law That Applies to Your Agreement." In *Run Them Sweet*, the choice-of-law provision was titled "Governing Law," designated Virginia as the required forum to resolve all disputes, and mandated that Virginia law applies to "[t]hese conditions and any contract made under them," language the Court concluded "'counsels in favor of a broad interpretation' because that combination "'manifests the intent to reduce uncertainty and proceed in one forum under one body of law.'" *Id*. at 467.

Capital One alternatively contends that Virginia's choice-of-law rules compels the application of Virginia substantive law to Plaintiffs' tort claims since each of their claims is premised on decisions made or performed in Virginia, where the last act necessary to impose tort liability occurred. *See Quillen v. International Playtex, Inc.*, 789 F.2d 1041, 1044 (4th Cir. 1986) ("The place of the wrong for purposes of the *lex loci delicti* rule, however, is defined as the place where "the last event necessary to make an act liable for an alleged tort takes place."). However correct that position may prove to be, without the benefit of fully-developed record, the Court cannot definitively decide which substantive law applies. The Court will, therefore, consider, for purposes of the Motions, each of the asserted claims under California, Florida, New York, Texas, Virginia, and Washington law**.**

B. Negligence

The Amended Complaint asserts a negligence claim under the law of each jurisdiction where a representative plaintiff resides. In moving to dismiss these claims, Defendants argue that the economic loss rule bars each of these claims and that Plaintiffs have otherwise failed to assert a cognizable injury or theory of causation.

1. Economic Loss Rule

Broadly recognized in each of the relevant states, the economic loss rule bars a plaintiff from recovering for purely economic losses under a tort theory of negligence. The rule, as applied, reflects the belief "that tort law affords the proper remedy for loss arising from personal injury or damages to one's property, whereas contract law and the Uniform Commercial Code provide the appropriate remedy for economic loss stemming from diminished commercial expectations without related injury to person or property." *In re Target Corp. Customer Data*

Sec. Breach Litig., 66 F. Supp. 3d 1154, 1171, 2014 U.S. Dist. LEXIS 175768, at *40 (citation omitted).

Plaintiffs contend that the economic loss rule does not apply under any of the applicable state laws for two reasons: (1) each state recognizes that the rule does *not* apply where the duty allegedly violated is an "independent duty" that does not arise from commercial or contractual expectations; and (2) there exists under certain states' law a so-called "special relationship" exception that removes their claims from the scope of the economic loss rule.

i. California

Under California's economic loss rule, "purely economic losses are not recoverable in tort." *NuCal Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013) (citation omitted). *See also Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 22 Cal. Rptr. 3d 352, 102 P.3d 268, 272 (Cal. 2004) ("The economic loss rule requires a purchaser to recover in contract for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise."). The purpose of the rule is to "prevent[ ] the law of contract and the law of tort from dissolving one into the other[,]" *Robinson*, 102 P.3d at 273 (citation omitted), and "courts will generally enforce the breach of a contractual promise through contract law, except when the actions that constitute the breach violate a social policy that merits the imposition of tort remedies." *Aas v. Superior Court*, 24 Cal. 4th 627, 643, 101 Cal. Rptr. 2d 718, 12 P.3d 1125 (Cal. 2000).

The economic loss rule also does not prevent recovery in tort if a "special relationship" exists between the plaintiff and the defendant. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 157 Cal. Rptr. 407, 598 P.2d 60, 63 (Cal. 1979). However, the *J'aire* special relationship exception appears to apply only if the contracts are for services, not goods. *R Power Biofuels, LLC v.*

Chemex LLC, 2016 U.S. Dist. LEXIS 156727, 2016 WL 6663002, at *5 (N.D. Cal. Nov. 11, 2016); *see also CoreLogic, Inc. v. Zurich Am. Ins. Co.*, 2016 U.S. Dist. LEXIS 121633, 2016 WL 4698902, at *5 (N.D. Cal. Sept. 8, 2016).

Plaintiffs allege that Capital One provided credit card services, Am. Compl. ¶¶ 18-27, which is an allegation in substance that there exists a contractual relationship between Plaintiffs and Defendants for services, not goods. *See* Cal. Com. Code § 2105(1) (a contract for "goods" involves the purchase or sale of "all things . . . which are movable at the time of identification to the contract for sale "); *TK Power, Inc. v. Textron, Inc.*, 433 F. Supp. 2d 1058, 1062 (N.D. Cal. 2006) (a contract for services involves the purchase of labor and the "knowledge, skill, and ability" of the contracting party). The issue then is whether the alleged Data Breach constitutes a breach of contract that "violate[s] a social policy that merits the imposition of tort remedies" or for the purposes of the *J'aire* exception, whether Plaintiffs have adequately pled a "special relationship." Because Plaintiff has alleged facts that make plausible its negligence claim under the *J'aire* exception, the Court does not address at this point whether Plaintiffs' negligence claim is otherwise cognizable under California law. [9]

Six factors determine whether a "special relationship" exists under *J'aire*:

> (1) the extent to which the transaction was intended to affect the plaintiff, (2) the foreseeability of harm to the plaintiff, (3) the degree of certainty that the plaintiff suffered injury, (4) the closeness of the connection between the defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct and (6) the policy of preventing future harm.

598 P.2d at 63.

[9] In *Aas v. Superior Court*, the California Supreme Court noted that "conduct amounting to a breach of contract becomes tortious when it also violates a duty independent of the contract arising from principles of tort law." 24 Cal. 4th at 643. At least one federal court has concluded that California law recognizes a legal duty independent of contract to provide reasonable security to PII it has received. *See Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 968 (S.D. Cal. 2014).

Plaintiff's allegations make plausible each of these factors. The contract entered into between the parties was for Plaintiffs' benefit; as part of the application process, customers were required to turn over their PII to Defendants in order to apply for and obtain credit card services and did so with the reasonable understanding and expectation that Defendants would adequately protect their PII and inform them of any misappropriation of that data; it was plainly foreseeable that customers would suffer injury if Defendants did not adequately protect the PII; and there is a sufficiently close connection between Defendants' conduct and the Plaintiffs' alleged injury that was traceable to and a result of Capital One's inadequate security. *See, e.g.*, Am. Compl. ¶¶ 212-219. Moreover, there is "moral blame" ascribable to Defendants' conduct: they allegedly knew that "their data security was inadequate," but "[did not] have the tools to detect and document intrusions or exfiltration of PII;" and they did not promptly notify Plaintiffs. Recognizing a cognizable claim furthers the policy of preventing future harms, as well as advances the California state policy regarding data protection expressed in California statutes such as the California Legal Remedies Act and the California Unfair Competition Law, discussed *infra*. Therefore, for all the above reasons, the "special relationship" exception applies; and the economic loss rule does not preclude Plaintiffs' tort claims under California law. *See In re: Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1133 (N.D. Cal. Mar. 9, 2018).

ii. Florida

In Florida, the economic loss rule only extends to product liability cases. *Tiara Condo Ass'n, Inc. v. Marsh & McLennan Companies, Inc.*, 110 So. 3d 399, 404 (Fla. 2013) (rejecting prior Florida rulings in which courts have applied the economic loss rule in non-products liability cases). It does not appear that any Florida court has considered whether a mass data breach falls

under the products liability category. At least one federal court applying Florida law has recognized that an entity that collects sensitive, private data from consumers and stores that data has an independent duty to protect that information. *See Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) (citing *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2011) (finding, implicitly, that healthcare providers owe patients a duty to protect their sensitive data) and *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1363 (S.D. Fla. 2015) (holding that ambulance service had a duty to exercise reasonable care in safeguarding and protecting the plaintiff's sensitive information)). It is also clear that Florida law does not require a plaintiff to prove that the conduct or acts giving rise to a tort claim are different from or additional to those acts that support the plaintiff's breach of contract claim. Indeed, "[w]here the acts constituting a breach of contract also amount to a cause of action in tort there may be a recovery of exemplary damages upon proper allegations and proof." *Griffith v. Shamrock Villag*e, 94 So. 2d 854, 858 (Fla. 1957); *accord Lewis v. Guthartz*, 428 So. 2d 222, 223 (Fla. 1982); *Nicholas v. Miami Burglar Alarm Co.*, 339 So. 2d 175, 178 (Fla. 1976).

Given the nature of a products liability claim and the appropriate entities against which a products liability claim is typically asserted, *see Samuel Friedland Family Enters. v. Amoroso*, 630 So. 2d 1067, 1068 (Fla. 1994) (product liability claims can be brought against manufacturers, retailers, wholesalers, distributors, and commercial lessors), Plaintiff has alleged facts that that make plausible that their claims against Capital One would be deemed to fall *outside of* Florida's economic loss rule. Therefore, the Court finds that Plaintiffs have asserted a cognizable negligence claim under Florida law.

iii. New York

Under New York law, "plaintiffs who have suffered 'economic loss,' but not personal or property injury, [are restricted to] an action for the benefits of their bargains." *Carmania Corp., N.V. v. Hambrecht Terrell Intern.*, 705 F. Supp. 936, 938 (S.D.N.Y. 1989). Thus, if "the damages suffered are of the type remediable in contract, a plaintiff may not recover in tort." *Id.*; *see also King Cnty., Wash. v. IKB Deutsche Industriebank AG*, 863 F. Supp. 2d 288, 302 (S.D.N.Y. 2012) ("[T]he economic loss doctrine serves two purposes: (1) it 'protect[s] defendants from disproportionate, and potentially limitless, liability'; and (2) it disentangles contract and tort law by restricting plaintiffs who suffer economic losses to the benefits of their bargains." (internal footnotes omitted)); *Ambac Assurance Corp. v. U.S. Bank Nat'l Ass'n*, 328 F. Supp. 3d 141, 159 (S.D.N.Y. 2018) (the "applicability of the economic loss rule outside the product-liability context from which it originated is doubtful.").

The New York Court of Appeals has not addressed whether the economic loss doctrine applies to data breach claims. However, federal district courts in New York, applying New York law, have declined to apply the economic loss doctrine to data breach claims. *See Rudolph v. Hudson's Bay Co.*, 2019 U.S. Dist. LEXIS 77665, *29-30, 2019 WL 2023713 (S.D.N.Y. May 7, 2019) ("In some circumstances, such as a construction accident that causes widespread damage and disruption, New York courts have engaged in "[p]olicy-driven line-drawing" to conclude that defendants owed a duty "to those who have . . . suffered personal injury or property damage," and not to those who suffered an "economic loss alone . . . . Defendants have not explained how such a limitation on negligence liability could apply to the data breach alleged in this case."); *see also Sackin v. Transperfect Global, Inc.*, 278 F. Supp. 3d 739, 749 (S.D.N.Y.

2017) (same). Taking its lead from those decisions, the Court likewise concludes that New York's economic loss rule does not bar Plaintiffs' tort claims.[10]

iv. Texas

Under Texas's economic loss rule, no duty in tort exists when plaintiffs have suffered only economic losses." *Meml. Hermann Healthcare Sys. Inc. v. Eurocopter Deutschland, GMBH*, 524 F.3d 676, 678 (5th Cir. 2008). Undecided is whether, under Texas law, Texas's economic loss rule applies to a data breach claim. *Cf. Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 423 (5th Cir. 2013) (data breach plaintiffs agreed that economic loss rule would bar negligence claim under Texas law); *In re Heartland Payment Sys., Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 568 (S.D. Tex. 2011) (same)

In *Thawar v. 7-Eleven, Inc.*, 165 F. Supp. 3d 524, 532 (N.D. Tex. 2016), the District Court concluded under Texas law that "if the [data protection policy] was a part of [plaintiff's] employment contract, then the economic loss doctrine may well bar her claim[,]" *Id*. at 532, but that "even where there is a contract between the parties, Texas courts will not apply the economic loss doctrine to bar a tort suit when the defendant is alleged to have breached 'an independent legal duty, separate from the existence of the contract itself.'" *Id*. at 532 (quoting *Sharyland Water Supply Corp. v. City of Alton*, 354 S.W.3d 407, 415 (Tex. 2011)); *see also Formosa Plastics Corp. USA v. Presidio Eng'rs & Contractors, Inc.*, 960 S.W.2d 41, 47 (Tex. 1998)). Because the District Court could not determine from the complaint whether such an independent duty existed, it refrained from dismissing the claim on that basis. *Id*. at 332-333.[11]

[10] The facts here are strikingly similar to those in *Rudolph*, where a group of hackers breached the payment-card databases of Saks Fifth Avenue and other companies owned by Hudson's Bay Co. 2019 U.S. Dist. LEXIS 77665, at *3.

[11] The district court in *Thawar* did not go into detail of the facts surrounding the incident.

It is unclear under Texas law what would qualify as an "independent duty" for the purposes of the economic loss rule. In *Buchanan v. Rose*, 159 S.W.2d 109, 138 Tex. 390, 391-392 (Tex. 1942), the Texas Supreme Court considered "whether one who drives over a bridge on a public road and thereafter discovers that such bridge, because of its defective condition, has broken down under the weight of his vehicle, without negligence on his part, is under any duty to give warning so as to prevent other travelers from being injured as a result of the broken bridge." 159 S.W.2d at 109. The Texas Supreme Court declined to recognize a duty to warn others of the defective bridge, whose deficiencies were not caused by the defendant's own negligence. It did acknowledge, however, that as a general proposition, "if a party *negligently* creates a dangerous situation it then becomes his duty to do something about it to prevent injury to others if it reasonably appears or should appear to him that others in the exercise of their lawful rights may be injured thereby." 159 S.W.2d at 110 (emphasis in original).

Here, plaintiffs have essentially alleged that by creating a so-called data lake without adequate safeguards to protect against hacking, Defendants have created a hazardous condition that threatened the Plaintiffs with foreseeable injuries. Based on the principle embraced in *Buchanan*, the Court concludes that if faced with this case, the Texas Supreme Court would recognize a duty separate and apart from the parties' contractual relationship; and for that reason, the Court will not dismiss Plaintiffs' negligence claim under Texas law based on the economic loss rule.

v. Virginia

Virginia courts routinely enforce the distinction between tort (*i.e.*, issues concerning safety of persons and property) and contract (*i.e.*, economic loss and the protection of bargained-for expectations) claims by applying Virginia's economic loss rule. *See, e.g., Selective Ins. Co. of*

the Se. v. Williamsburg Christian Acad., 2020 U.S. Dist. LEXIS 76433, at *15 (E.D. Va. April 30, 2020); *1004 Palace Plaza, LLC v. Ebadom Food, LLC*, No. 1:18-cv-1376, 2019 U.S. Dist. LEXIS 118320, at *5-6 (E.D. Va. July 15, 2019) ("Virginia courts diligently protect the line between claims arising in contract and those in tort in order to prevent every breach of contract from being turned into a tort."); *Metro. Life Ins. Co. v. Gorman Hubka*, 2016 U.S. Dist. LEXIS 193165, at *9 (E.D. Va. Mar. 28, 2016). And as the Supreme Court of Virginia has explained, the economic loss doctrine reasons that:

> The law of torts is well equipped to offer redress for losses suffered by reason of a breach of some duty imposed by law to protect the broad interests of social policy. Tort law is not designed, however, to compensate parties for losses suffered as a result of a breach of duties assumed only by agreement. That type of compensation necessitates an analysis of the damages which were within the contemplation of the parties when framing their agreement. It remains the particular province of the law of contracts.

Sensenbrenner v. Rust, Orling & Neale, Artichitects, Inc., 236 Va. 419, 425, 374 S.E. 2d 55 (Va. 1988).

Related to the economic loss doctrine, the source of duty rule recognizes that tort recovery should not be allowed when the duty stems from (and solely because of) a contract. And Virginia courts have applied this rule regularly. *See Napier v. PSC & Son Builders, Inc.*, 95 Va. Cir. 134, 136 (Va. Cir. 2017) (applying the economic loss doctrine/source of duty rule to bar fraud and negligence claims when they were premised on the same conduct as a breach of contract claim, stating that "the plaintiff has sued for the exact same acts and damages under both breach of contract and negligence"); *Filak v. George*, 267 Va. 612, 618, 594 S.E. 2d 610 (Va. 2004) ("[L]osses suffered as a result of the breach of a duty assumed only by agreement, rather than a duty imposed by law, remain the sole province of the law of contracts . . . . [W]hen a plaintiff alleges and proves nothing more than disappointed economic expectations . . . the law

of contracts, not the law of torts, provides the remedy for such economic losses."). Nevertheless, when a tort duty exists alongside, or in addition to, a contractual right or obligation, Virginia courts have allowed an action to proceed with respect to both claims. *See, e.g.*, *JPMCCM 2010-C1 Aquia Office LLC v. Mosaic Aquia Owner*, LLC, No. CL17-250, 2019 Va. Cir. LEXIS 74, at *15-16 (Va. Cir. Jan. 15, 2019) ("Only in certain circumstances will a single act or omission support causes of action both for breach of contract and for breach of a duty arising in tort . . . . The salient issue is whether [Defendant] owed [Plaintiff] a common law duty, independent of their contractual agreements."); *Richmond Metro. Auth. v. McDevitt St. Bovis, Inc.*, 256 Va. 553, 558 (Va. 1998) ("If . . . the relation of the plaintiff and the defendants be such that a duty arises from that relationship, irrespective of the contract, to take due care, and the defendants are negligent, then the action is one of tort."). Thus, the source of duty rule permits a party to assert a tort claim, in spite of the presence of a contract, if the underlying duty arises independent of any contractual duties or covenants.

Two Virginia cases have tangentially addressed whether there is a duty to protect PII independent of any duty arising from contract, *Parker v. Carilion Clinic*, 819 S.E.2d 809 (Va. 2018) and *Deutsche Bank Nat'l Trust Co v. Buck*, No. 3:17-cv-833, 2019 WL 1440280 (E.D. Va. Mar. 29, 2019). In *Parker*, the medical clinic's employees stole a laptop that contained confidential patient information; and the Supreme Court of Virginia held that the clinic did not have an independent common law duty to protect patient information from unauthorized access in that manner. *Id*. at 347 (observing that no Virginia court "ha[d] ever imposed a tort duty on a healthcare provider to manage its confidential information systems so as to deter employees from willfully gaining unauthorized access to confidential medical information."). Months after *Parker* was decided, this Court in *Deutsche Bank Nat'l Trust Co v. Buck* declined to recognize

under Virginia law a common law duty on the part of a closing agent in a real estate transaction to protect against an electronic data breach.[12] 2019 U.S. Dist. LEXIS 54774, at *13 (E.D. Va. Mar. 29, 2019) (Lauck, J.).

The alleged facts here are fundamentally different than in either *Parker* or *Buck*. Here, Capital One solicited customers' PII as a pre-condition for considering whether to provide credit card services to that customer; it then continued to possess and aggregate that PII with other customer's PII for its own business purposes, beyond those pertaining to the particular customer whose PII was obtained. Am. Compl. ¶¶ 26-34. As a result, Capital One created a massive concentration of PII, a "data lake," in which Capital One "mines [customers'] data for purposes of product development, targeted solicitation for new products, and target marketing of new partners—all in an effort to boost its profits." *Id.* ¶ 28. This undertaking was foreseeably vulnerable to a data attack, evidenced most clearly by Capital One's and Amazon's joint efforts to develop a security product (Cloud Custodian) whose purpose was to protect against these vulnerable flaws. *Id.* ¶¶ 44-59, 161. Indeed, Capital One acknowledged and anticipated attempts to gain unauthorized access and use of that PII, taking steps to protect against it, albeit inadequately. *Id.* ¶¶ 54-59.

Virginia has recognized the concept of assumption of duty: "one who assumes to act, even though gratuitously, may thereby become subject to the duty of acting carefully, if he acts at all." *Kellermann v. McDonough*, 278 Va. 478, 493-494, 684 S.E.2d 786, 791 (Va. 2009); *see also Terry v. Irish Fleet, Inc.*, 296 Va. 129, 138, 818 S.E.2d 788, 793 ("As a general proposition,

[12] In *Buc*k, a non-party hacked and obtained information about the real estate transaction from the closing agent, Altisource, a third-party defendant who had been engaged by Deutsche Bank to close the transaction, and with that hacked information mimicked Altisource's e-mail tricking Buck into sending the closing funds to it, not Altisource. *Id.* at *2. At issue were the equitable indemnification and contribution claims of Deutsche Bank against Altisource.

a duty that does not otherwise exist may be impliedly assumed from the defendant's conduct.") (citing 2 Dan B. Dobbs et al., The Law of Torts § 410, at 671 (2011) (recognizing that an implied undertaking may give rise to an assumed duty)). Thus, by way of example, the Supreme Court of Virginia has recognized that an assumed duty may be undertaken gratuitously by a motorist to another motorist or a pedestrian when he signals to the other motorist or pedestrian that it is safe to proceed. *See Ring v. Poelman*, 240 Va. 323, 327, 397 S.E.2d 824, 826 (1990) (noting that an assumed duty could arise based on evidence that motorist signaled to another motorist that it was safe to proceed, but holding no evidence of proximate cause); *Cofield v. Nuckles*, 239 Va. 186, 192-93, 387 S.E.2d 493, 496-97 (1990) (noting that an assumed duty could arise based on evidence that the motorist signaled to a pedestrian that it was safe to proceed, but holding no evidence of breach of duty); *Nolde Bros. v. Wray*, 221 Va. 25, 28-29, 266 S.E.2d 882, 884 (Va. 1980) (driver's gesture could not be construed as a signal for the plaintiff to proceed across lanes of highway so driver did not assume a duty to the plaintiff).

Likewise, the Supreme Court of Virginia has recognized the assumption of a duty of care in the medical care context. *See Didato v. Strehler*, 262 Va. 617, 629, 554 S.E.2d 42, 48 (Va. 2001) (citing Restatement (Second) of Torts § 323) (finding that "the plaintiffs pled sufficient facts which, if proven at trial, would permit the finder of fact to conclude that the defendants assumed the duty to convey to the plaintiffs the correct results of their daughter's test, which indicated that she carried the sickle cell trait."); *Fruiterman v. Granata*, 276 Va. 629, 645, 668 S.E.2d 127, 136 (Va. 2008) (acknowledging principle but holding that physician did not undertake to provide health care). Across each of these cases, the Supreme Court of Virginia either "explicitly or implicitly required the defendant to 'personally engage in some affirmative act amounting to a rendering of services to another.'" *Bosworth v. Vornado Realty L.P.*, 83 Va.

Cir. 549, 557 (Va. Cir. 2010) (citing *Fruiterman*, 668 S.E.2d at 137). Whether, based on the facts alleged, the law will recognize an assumed duty in tort is a question of law. *Terry*, 818 S.E.2d at n.6.[13]

This case does not fit within the narrow band of Virginia's decided assumption of duty cases. But nothing in the cases that have applied the voluntary undertaking doctrine has expressly limited the doctrine only to the wrongful death, wrongful birth, or certain driving-related torts; and the Court concludes that if confronted with this case, the Supreme Court of Virginia would recognize an assumed duty, owed by Defendants to Plaintiffs.

As articulated by the Supreme Court of Virginia in *Burns*, liability under the voluntary duty doctrine is in lockstep with § 323 of the Restatement (Second) of Torts, which provides that:

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for physical harm resulting from his failure to exercise reasonable care to protect his undertaking, if
>
> (a) his failure to exercise reasonable care increases the risk of such harm, or
> (b) he has undertaken to perform a duty owed by the other to the third person, or
> (c) the harm is suffered because of reliance of the other or the third person upon the undertaking.

Burns, 727 S.E.2d at 644. Thus, a party can be subject to liability provided that the plaintiff prove that a party undertook an affirmative course of action and then either: (1) the defendants failed to exercise reasonable care in performing the undertaking thus increasing the risk of the

[13] Importantly, there is a distinction between this question (of law) and the separate question (of fact) regarding whether, based on the facts alleged, a defendant, by its conduct, in fact assumed a duty. *See Burns v. Gagnon*, 283 Va. 657, 672, 727 S.E.2d 634, 643 (Va. 2012) ("[W]hen the issue is not whether the law recognizes a duty, but rather whether the defendant by his conduct assumed a duty, the existence of that duty is a question for the fact-finder.") (citing *Kellermann*, 684 S.E.2d at 791-92 and *Didato*, 554 S.E.2d at 48)).

harm; (2) that defendants undertook to perform a duty owed by another to a third party; or (3) that the harm was a result of either party's reliance upon the defendant's undertaking." *Id.*

Here, the Amended Complaint alleges that Capital One and Amazon voluntarily undertook a duty to protect its customers' PII manifested via its affirmative acts and representations regarding its ability and responsibility to render adequate data protection services to its customers. Am. Compl. ¶¶ 96-98. The Amended Complaint further alleges that Capital One and Amazon, aware of the vulnerabilities and risks associated with their servers on which they stored Plaintiffs' PII, failed to take reasonable care to protect Plaintiffs' PII from unauthorized access, increasing the risk of harm. *Id.* ¶¶ 50-59, 60-75, 100-108. Together, these allegations plausibly satisfy the voluntary undertaking doctrine under Virginia law. Indeed, finding that a duty exists here would not in concept represent a marked deviation from existing Virginia case law on the subject, particularly considering the nature of the risks involved, the foreseeability of those risks, Defendants' alleged knowledge and awareness of those risks, the reasonableness of the measures allegedly available to adequately protect against these risks, and the attendant damages that followed. Overall, the nature of the context here is not altogether qualitatively different than those contexts Virginia courts have found an assumed duty of care to exist.

For the above reasons, Plaintiffs have alleged facts that make plausible negligence claims under Virginia law that would not be barred under the economic loss rule.

vi. Washington

Where a plaintiff's claims arguably arise out of a contractual relationship, Washington courts apply the "independent duty doctrine," under which the plaintiff may bring a tort claim only if the injury "traces back to the breach of a tort duty arising independently of the terms of

the contract." *Affiliated FM Ins. Co. v. LTK Consulting Servs., Inc.*, 243 P.3d 521, 526 (Wash. 2010). "To determine whether a duty arises independently of the contract, [the Court] must first know what duties have been assumed by the parties within the contract. If a contract term (such as a term defining the scope of the parties' contractual duties) is ambiguous, the [Court] must ascertain the intent of the parties." *Donatelli v. D.R. Strong Consulting*, 312 P.3d 620, 627 (Wash. 2013).

In *Donatelli*, the Washington Supreme Court explained that the goal of the independent duty doctrine is to "maintain the boundary between torts and contract." *Id*. at 623. To do so, the court explained that the doctrine asks: (1) what the terms of the contract are, (2) whether the duties alleged have been assumed by the parties within the contract, and (3) determine whether a duty arises independently of the contract. *Id*. at 624. And as applied in *Donatelli*, the Washington Supreme Court found that the trial court correctly denied the defendant's motion for summary judgment as to plaintiff's negligent misrepresentation claim because the record did *not* establish the duties that fell within the contract, *Id*. at 625, and defendants *did* have a duty to avoid misrepresentations, independent of the scope of the contract, *Id*. at 627.

Here, as with Texas and Virginia law, the application of the economic loss rule will turn on what qualifies as a duty independent of the contract, specifically, whether there exists an independent duty to protect PII under the alleged facts in this case. At least one Washington court has held that "the failure to implement adequate data security measures does *not* implicate a legal duty on its own." *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813 BHS, 2018 U.S. Dist. LEXIS 53411, 2018 WL 1532671, at *5 (W.D. Wash. Mar. 29, 2018) (applying Washington law). And in the absence of "clear Washington authority" suggesting otherwise, "the Court declines to extend Washington's 'special relationship' doctrine to include

relationships between businesses and consumers when the parties' transaction involves the disclosure of private information." *Id*. at *5-6. Based on the current state of Washington law, the Court concludes that Plaintiffs' Washington law negligence claim does not survive application of that state's economic loss rule.[14]

2. Merits

Having determined that the laws of California, Florida, Texas, New York, and Virginia do not bar Plaintiffs' negligence claims, the Court has considered whether Plaintiffs' have adequately stated those claims. In that regard, the Defendants argue that Plaintiffs have failed to adequately allege either injury or proximate causation. [Doc. 387] at 13-23; [Doc. 390] at 12-14. The Court disagrees.

i. Alleged Harms

Focusing on Virginia law, Defendants contend that no theory of damages proffered by Plaintiffs is sufficient to sustain their negligence claim.

Plaintiffs allege five types of harm that they contend are sufficient to allege damages: (1) they were subject to an increased risk of future identity theft due to the exposure of their personal

[14] Plaintiffs concede that Washington law has not recognized a duty to provide adequate data security to protect customers from a data breach. [Doc. 427] at n.11. Nonetheless, Plaintiffs argue that Washington would, under the facts of this case, recognize such a duty based on *Meneely v. S.R. Smith, Inc.*, 101 Wn. App. 845, 859, 5 P. 3d 49, 58 (Wash. Ct. App. 2000) ("SPI's voluntary undertaking to promulgate minimum safety design standards made it foreseeable that harm might result to the consumer if it did not exercise due care.") (internal quotations and citation omitted))). *Meneely*, however, was decided within the context of the voluntary rescue doctrine. *See id*. at 859 ("We hold the foregoing facts fall squarely within the voluntary rescue doctrine."). The voluntary rescue doctrine states that tort liability "may arise if a defendant takes steps to assist a person in need and acts negligently in rendering that assistance." *Folsom v. Burger King*, 135 Wn.2d 658, 675 958 P.2d 301 (1998). That, however, is conceptually distinct from a voluntary undertaking doctrine, which Plaintiffs rely on here and which the *Meneely* court expressly declined to apply after noting that the concept "has not yet been adopted by a Washington court." *Meneely*, 101 Wn. App. at n.4 (citing Restatement (Second) of Torts § 324A).

information "after the Data Breach," Am. Compl. ¶¶ 18-27; (2) they incurred expenses or took efforts to mitigate the consequences of the Cyber Incident, *id*; (3) they have lost "the inherent value" of their stolen personal information, *id*., ¶ 142; and (4) they "did not receive the benefit of their bargain with Capital One," *id*. ¶ 145. A subset of several Plaintiffs also allege they experienced actual or attempted identity theft or fraud at some point "after the Data Breach." *Id*. ¶¶ 19-21, 23-24, 26-27.

1. Actual Fraud or Imminent Risk of Fraud

To the extent certain Plaintiffs allege that they suffered monetary losses in connection with actual fraudulent charges, including unauthorized charges on their accounts, theft of their personal financial information, and costs associated with the detection and prevention of identity theft, these allegations of damages are sufficient to survive a motion to dismiss. *See* Am. Compl. ¶¶ 19-21, 23-24, 26-27; *see also Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018) (finding that because party suffered actual harm actual harm in the form of identity theft and credit card fraud, there was a concrete injury); *cf. Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (because "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," plaintiffs failed to assert Article III standing). Nevertheless, Defendants contend that because Plaintiffs solely allege that they experienced identity theft or fraud or unauthorized activity on their accounts sometime *after* the Data Breach as well as not alleging precisely *what* the hacker (Paige Thompson) did with the stolen PII, they have failed to plausibly allege the required connection to the Data Breach sufficient to support any alleged damages. [Doc. 463] at 4-5.

Virginia law requires that a plaintiff show causation "is a probability rather than a merely possibility," *Atrium Unit Owners Ass'n v. King*, 585 S.E.2d 545, 558 (Va. 2003). Drawing all inferences in favor of Plaintiffs, Plaintiffs have alleged facts that make plausible their actual fraud or risk of imminent fraud theory of damages. As alleged, the hacker (Paige Thompson) successfully extracted their PII from Defendants' servers; posted instructions about how to access the stolen data on Github, a software development platform; and after these events, several Plaintiffs suffered actual misuse of their PII, thus raising the plausible inference that Thompson shared the information with others or enabled others to receive that information and plausibly connecting the Data Breach to Plaintiffs' alleged injuries. Am. Compl. ¶¶ 18-27, 61, 69. Based on these allegations, it is also plausibly alleged that there exists, beyond the speculative level, the imminent threat of identify threat. *Cf. In re Marriott Int'l, Inc.*, 440 F. Supp. 3d 447, 462-65 (D. Md. 2020) ("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 . . . [I]n these circumstances the remaining [] Plaintiffs do not have to wait until they, too, suffer identity theft to bring their claims to this court.").[15]

2. Lost Value of Plaintiffs' PII

[15] Because the Plaintiffs have satisfactorily alleged that the risk of harm has occurred or is, at the least, sufficiently imminent, the time and expense incurred as a reasonable reaction to a risk of this harm constitutes plausible damages. *See* Restatement (Second) of Torts § 919(1) (1979) ("One whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened."); *cf. Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013) (rejecting recovery for costs incurred as a "reasonable reaction" to a risk of harm because the harm the plaintiffs seek to avoid was not sufficiently imminent); *Beck*, 848 F.3d at 274 (same). Here, several representative plaintiffs incurred these costs, which the Court finds are sufficient to establish damages under state law. *See* Compl. ¶¶ 19-21, 23, 24, 26.

Plaintiffs separately allege—as an alternative basis for damages—that their PII and the intangible products related thereto (*e.g.*, credit scores, credit limits and payment history) have significant value, which is now diminished because of its disclosure, particularly to those who may use that PII for nefarious purposes. Am. Compl. ¶¶ 131-133.[16] Plaintiff contend in that regard that because there is a market for the sale and purchase of consumer data, the unwanted exposure of their personal information following the Data Breach effectively reduces the value of their data given its susceptibility to fraudulent purposes. Plaintiffs contend that they are entitled to recover for this unwanted exposure, ostensibly measurable in some form.

A growing number of courts recognize a loss in value as a cognizable injury for the purposes of establishing Article III standing. *See, e.g., In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at 462-65 (collecting cases). Nevertheless, Plaintiffs have not plausibly alleged that that they have been injury under that theory of damages. Even assuming that Plaintiffs' PII has monetary value, Plaintiffs do not allege any facts explaining *how* their PII became less valuable as a result of the breach. For instance, they are no allegations that Plaintiff attempted to sell their information and were refused a sale because of or related to their PII's prior exposure arising from the Data Breach. Nor is there any allegation that Plaintiff have attempted to purchase goods or services, which requires the exchange of their PII, and Plaintiffs were denied receipt of that good or service or were only offered less-than-desirable terms because of their PII's prior exposure through the Data Breach. As other courts have concluded with respect to similar claims, Plaintiffs have therefore failed to plausibly allege damages based on the lost or reduced value of their PII. *See, e.g., In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954 (D. Nev. 2015) (citing *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 660 (S.D. Ohio

[16] Seven of the representative Plaintiffs allege their PII was used for fraudulent purposes.

2014) (rejecting a similar argument because the named plaintiffs failed to allege that the data security breach actually prevented them from selling their information at the price they claimed the data was worth) and *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014)).

3. Plaintiffs' Failure to Receive the Benefit of their Bargain

Plaintiffs also contend that they were harmed by a "loss of the benefit of the bargain" based on Capital One's failure to provide sufficient data security to protect Plaintiffs' PII and that, in return, Plaintiffs were harmed vis-a-vis their "overpaying for Capital One's services." [Doc. 427] at 16. In that regard, Plaintiffs contend that they place significant value on data security, Am. Compl. ¶¶ 16, 143; that companies with (perceived) robust data security practices, such as Capital One, can command higher prices based on these data security practices, *id.* ¶ 144; and that had Plaintiffs known the truth about Capital One's inadequate security practices, it would not have purchased Capital One's services or, at the very least, would have insisted on paying lower prices, *id.* ¶¶ 145, 187, 226.

To date, Virginia 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; and Plaintiffs cite no case authority for permitting recovery of "lost benefit of the bargain damages' on a negligence claim.[17] Moreover, despite this courts' conclusion that the

[17] In the cases Plaintiffs do cite in support of this damages theory, none were decided in the context of a state law negligence claim. *See, e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1130 (N.D. Cal. 2018) (concluding, under Article III, 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, under the New York General Business Law, who alleged they had contracted for "reasonable and adequate security

economic loss or source of duty rules do not otherwise bar Plaintiff's tort claims, it nevertheless remains true that "[t]he controlling policy consideration underlying the law of contracts is the protection of expectations bargained for." *Sensenbrenner*, 374 S.E.2d at 58. This is true in other jurisdictions as well. *See, e.g.*, *Career Care Inst., Inc. v. Accrediting Bureau of Health Educ. Schs., Inc.*, 2009 U.S. Dist. LEXIS 23651, at *15-16, 2009 WL 742532 (E.D. Va. 2009) (Trenga, J.) (citing *Seely v. White Motor Co.*, 63 Cal. 2d 9, 18, 403 P.2d 145 (Cal. 1965)) (under California law, economic damages representing the lost benefit of a bargain are not recoverable under tort law.)

For the above reasons, Plaintiffs have failed to allege cognizable damages under their negligence claims based on the benefit of the bargain theory.

ii. Proximate Cause

Defendants contend that Paige Thompson's intervening hack broke the causal chain between Defendants' alleged negligence and the Data Breach. [Doc. 387] at 22.[18]

Under Virginia law, "[t]he proximate cause of an event is that act or omission which, in natural and continuous sequence, unbroken by an efficient intervening cause, produces the event, and without which that event would not have occurred." *Beverly Enterprises-Virginia v. Nichols*,

---

measures" that Anthem failed to deliver, causing plaintiffs to overpay for their health insurance). The courts that have, have rejected the theory. *See also Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13 (D.D.C. Jan. 30, 2019) (concluding that plaintiff failed to plausibly plead economic injury-in-fact based on an "overpayment" theory under DC law) (citing *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014) and *Austin-Spearman v. AARP & AARP Servs. Inc.*, 119 F. Supp. 3d 1, 13-14 (D.D.C. 2015)).

[18] Capital One also argues that proximate causation requires a special relationship between itself and Plaintiffs, which does not exist here. [Doc. 387] at 22. While it is true that a special relationship is sometimes required to trigger certain duties, such as duty to warn or protect another from the criminal acts of a third person, *see, e.g., A.H. v. Church of God in Christ, Inc.*, 297 Va. 604, 639, 831 S.E.2d 460, 480 (Va. 2019) , a special relationship is not required to recover for injuries proximately caused by the breach of Defendants' duty to provide reasonable data security for Plaintiffs' PII against hacks of the sort that, as alleged, caused the Data Breach.

247 Va. 264, 269, 441 S.E.2d 1, 4 (Va. 1994) (quoting *Coleman v. Blankenship Oil Corp.*, 221 Va. 124, 131, 267 S.E.2d 143, 147 (Va. 1980)). That said, there may be more than one proximate cause of an event. *Williams v. Le*, 276 Va. 161, 167, 662 S.E.2d 73, 77 (Va. 2008). And whether a subsequent proximate cause relieves a defendant of liability turns on whether the "negligence intervening between the defendant's negligent act and the injury . . . so entirely supersede[s] the operation of the defendant's negligence that it alone, without any contributing negligence by the defendant in the slightest degree, causes the injury." *Atkinson v. Scheer*, 256 Va. 448, 454, 508 S.E.2d 68, 71 (Va. 1998). Thus, a superseding cause of an injury 'constitutes a new effective cause and operates independently of any other act, making it and it only the proximate cause of injury.'" *Kellermann*, 684 S.E.2d at 794.

But not every intervening cause is a superseding cause; and in order to relieve a defendant of liability for his negligence, the negligence intervening between the defendant's negligence and the injury "must so entirely supersede the operation of the defendant's negligence that it alone, without the defendant's [negligence contributing] thereto in the *slightest degree*, produces the injury." *Richmond v. Gay*, 103 Va. 320, 324, 49 S.E. 482, 483 (Va. 1905) (emphasis added). In addition, an intervening cause is not a superseding cause if it was "put into operation by the defendant's wrongful act or omission." *Jefferson Hospital, Inc. v. Van Lear*, 186 Va. 74, 81, 41 S.E.2d 441, 444 (Va. 1947).

Based on the above principles, the Court cannot conclude that, as a matter of law, Thompson's conduct sufficiently superseded Defendants' alleged negligence. Plaintiffs allege that Capital One knew it was a target of cyber hacks, Am. Compl. ¶¶ 90-97; that it had been breached before, *id*. ¶ 95; that it had recognized the risk of a data compromise, *id*. ¶¶ 98-100; and in fact knew of the very vulnerability that was ultimately exploited by Thompson, *id*. ¶¶ 46-61.

As for Amazon, Plaintiffs allege that it jointly-developed Cloud Custodian, which failed to remedy the well-known vulnerabilities on Amazon's system, it failed to implement adequate security systems, protocols and practices to protect Plaintiffs' PII from those known vulnerabilities or maintain a security system sufficiently consistent with relevant industry standards. *Id*. ¶¶ 56-58, 59-60. Based on these allegations, Defendants' negligent conduct foreseeably "put into operation" the sequence of events that made Thompson's attack possible; and therefore, as alleged, Plaintiffs have plausibly alleged, in effect, that Thompson's criminal conduct was not the superseding cause of Plaintiff's injuries, but rather a contributing factor, predicated on the Defendant's own negligence that allowed the Data Breach to take place.[19]

C. Negligence *per se*

[19] The Court reaches this same conclusion under California, Florida, New York, and Texas law. *See Schrimscher v. Bryson*, 58 Cal. App. 3d 660, 664, 130 Cal. Rptr. 125, 127 (Cal. 2d Dist. App. 1976) ("The general test of whether an independent intervening act, which operates to produce an injury, breaks the chain of causation is the foreseeability of that act. . . [And] an act is not foreseeable and thus is a superseding cause of the injury if the independent intervening act is highly unusual or extraordinary, not reasonably likely to happen . . .) (internal quotation and citation omitted); *Vining v. Avis Rent-A-Car Sys.*, 354 So. 2d 54, 55-56 (Fla. 1977) ("[I]f an intervening criminal act is foreseeable, the chain of causation is not broken and thus the original negligence may be the proximate cause of the damages sustained."); *Maheshwari v. City of New York*, 2 N.Y.3d 288, 295, 810 N.E.2d 894, 898 (N.Y. 2004) ("Where the acts of a third person intervene between the defendant's conduct and the plaintiff's injury, the causal connection is not automatically severed. In such a case, liability turns upon whether the intervening act is a normal or foreseeable consequence of the situation created by the defendant's negligence. An intervening act may break the causal nexus when it is extraordinary under the circumstances, not foreseeable in the normal course of events, or independent of or far removed from the defendant's conduct.") (citing *Deridian v. Felix Const. Corp*., 51 N.Y.2d 308, 315, 414 N.E.2d 666, 670 (N.Y. 1980) (internal quotations omitted)); *Stanfield v. Neubaum*, 494 S.W.3d 90, 99 (Tex. 2016) ("An intervening cause supersedes the original negligence when it alters the natural sequence of events, causes injuries that would not otherwise have occurred, was *not* brought into operation by the original wrongful acts of the defendant, and operates entirely independently of the defendant's negligent **act** or omission.") (emphasis added) (internal quotations and citations omitted). Separately, the courts to have addressed this issue in the data breach context have concluded, albeit under different law, the same. *See, e.g.*, *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 U.S. Dist. LEXIS 65111, 2016 WL 2897520, at *1 (N.D. Ga. 2016) (Georgia law) ("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.").

Plaintiffs allege Capital One's violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and the Gramm-Leach-Bliley Act's ("GLBA") Safeguards Rule results in negligence *per se* liability. Am. Compl. ¶¶ 172-180. Defendants move to dismiss this claim on two grounds. *First*, they contend that because neither has a common law duty to safeguard PII, any reference to a standard of care established by a federal statute or rule is irrelevant. And *second*, because neither Section 5 of the FTC Act nor the GLBA's safeguards rules was enacted for "public safety," negligence *per se* liability cannot follow. Plaintiffs concede that they do not state a claim for negligence *per se* under the California, Washington, Florida, or Texas law, [Doc. 427] at n.13; and the Court will only review Plaintiffs' negligence *per se* claim under New York and Virginia law.

1. New York

Under New York law, the unexcused omission or violation of a duty imposed by statute for the benefit of a particular class is negligence itself." *Timperio v. Bronx-Lebanon Hosp. Ctr.*, 384 F. Supp. 3d 425, 434 (S.D.N.Y. 2019). As such, New York courts have routinely held that a violation of a state statute, which properly imposes a duty of care, can sustain a claim for negligence *per se*. *Elliott v. City of New York*, 95 N.Y.2d 730, 734, 747 N.E.2d 760, 762 (N.Y. 2001) ("As a rule, violation of a State statute that imposes a specific duty constitutes negligence *per se*, or may even create absolute liability.") And there is no reason under New York law for distinguishing between state and federal statutes as the basis for a negligence per se claim. *See Wedlock v. Troncoso*, 185 Misc. 2d 432, 436, 712 N.Y.S.2d 328, 332 (Cty. Sup. Ct. 2000) ("a violation of a State or Federal statute constitutes negligence *per se*").

Under New York law, negligence *per se* exists "if a statute is designed to protect a class of persons, in which the plaintiff is included, from the type of harm which in fact occurred as a

result of its violation, the issues of the defendant's duty of care to the plaintiff and the defendant's breach of that duty are conclusively established upon proof that the statute was violated." *German by German v. Fed. Home Loan Mortgage Corp.*, 896 F. Supp. 1385, 1396 (S.D.N.Y. 1995); *see also Coene v. 3M Co. ex rel. Minnesota Min. & Mfg. Co.*, 2015 WL 5773578, at *5 (W.D.N.Y. Sept. 30, 2015). reasoning in these opinions.

Section 5 of the FTC Act is a statute that creates enforceable duties, and 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.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases. *Id.* ("The Federal Trade Commission Act prohibits 'unfair or deceptive acts or practices in or affecting commerce.'" (citing 15 U.S.C. § 45(a)). *See also LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018) (affirming that the FTC's prosecution of a company for inadequate data security measures with respect to health data is appropriate under Section 5 but finding that the cease and desist order issued by the FTC was unenforceable because it did not direct LabMD to cease committing the specific unfair act or practice alleged in the action which gave rise to the enforcement action).

Several federal district courts have recognized negligence *per se* claims based on alleged violations of Section 5 of the FTC act. In doing so, these courts have found, notably in the data breach context, that not only does the underlying substantive law permit a negligence *per se* action to rest on a violation of federal statute, but also that plaintiffs whose information was allegedly compromised by a data breach fit within the class of plaintiffs sought to be protected from the type of harm proscribed by the statute. *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 U.S. Dist. LEXIS 131140, 2018 WL 2128441, at *14 (N.D. Ga. Mar. 5, 2018); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 2016 U.S. Dist. LEXIS 65111, 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 U.S. Dist. LEXIS 20754, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017), report and recommendation adopted, 2017 U.S. Dist. LEXIS 48339, 2017 WL 1190500 (W.D. Pa. Mar. 31, 2017) (following *Home Depot* and declining to dismiss Pennsylvania negligence *per se* claim based on Section 5 of the FTC Act). The Court agrees with these decisions and because New York law would permit the Plaintiffs to assert a negligence *per se* claim premised on a federal statute and because Plaintiffs have adequately done so here—importing the standard of care from the FTC Act—Plaintiffs have plausibly alleged a claim for negligence *per se* under New York law.

2. Virginia

To sue for negligence *per se* in Virginia, a plaintiff must show that (1) "the defendant violated a statute enacted for public safety," (2) that he "belong[s] to the class of persons for whose benefit the statute was enacted," (3) "that the harm that occurred was of the type against which the statute was designed to protect," and (4) that "the statutory violation [was] a proximate cause of" his injury. *Collett v. Cordovana*, 290 Va. 139, 148, 772 S.E.2d 584, 589 (Va. 2015). Here, the issue reduces to whether the FTC and the GLBA are statutes enacted for "public safety." In Virginia, a "statute enacted for public safety generally is designed to afford protection to the public against careless or reckless acts which may result in *bodily injury* or *property damage*." *Tidewater Marina Holdings, LC v. Premier Bank, Inc.*, No. CL12-89, 2015 WL 13801664, at *2 (Va. Cir. Ct. Aug. 7, 2015) (emphasis added).

Section 5 of the FTC Act was intended to prevent unfair and deceptive trade practices, *see* 15 U.S.C. § 45 ("The [Federal Trade] Commission is hereby empowered and directed to prevent . . . unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.") while the GLBA was designed to encourage financial institutions to "respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information," 15 U.S.C. § 6801.

To date, no Virginia court has held that a state negligence *per se* claim can be based on either the FTC or GBLA, and based on current Virginia law, the Court concludes that the Supreme Court of Virginia would not recognize such a claim.[20] Neither the FTC nor the GLBA is expressly aimed at protecting public safety, as that term is applied under Virginia law. Indeed, this Court has previously rejected the view that statutes aimed at protecting society from fraud and other dishonest conduct, while having a facial impact on the public, is not the type of regulation that can support a negligence *per se* claim. *See Zuberi v. Hirezi*, 2017 U.S. Dist. LEXIS 14150, at *16, 2017 WL 436278 (E.D. Va. 2017) ("Therefore, plaintiffs' negligence *per se* claim based on the real estate licensing laws is also deficient."); *Evans v. Evans*, 280 Va. 76, 695 S.E.2d 173, 177 (Va. 2010) (a claim of negligence *per se* based on a violation of a state statute requiring child restraint devices in automobiles was impermissible.); *cf. Schlimmer v. Poverty Hunt Club*, 597 S.E.2d 43, 46 (Va. 2004) (firearm regulations qualify as public safety laws).

Therefore, for the foregoing reasons, the Court concludes that Plaintiffs have failed to state a claim for negligence *per se* under Virginia law.

[20] In support of its position that either the FTC and the GLBA can provide a standard of care in negligence *per se* suits, Plaintiff cites only to cases decided under non-Virginia state laws. *See* [Doc. 427] at 29.

D. Breach of Confidence

Plaintiffs allege Capital One is liable for "breach of confidence" in taking possession of Plaintiffs' PII in confidence and providing inadequate data security measures to prevent its disclosure. Am. Compl. ¶¶ 204-13. According to Plaintiffs, this tort, which involves the unconsented public disclosure to a third-party of nonpublic information, is a cognizable tort under each of the relevant states. [Doc. 427] at 29-30 (citing *McGuire v. Shubert*, 722 A.2d 1087, 1091 (Pa. Super. Ct. 1998) (recognizing duty between banker and customer that "banker will not divulge to third persons, without the consent of the customer . . . any information relating to the customer acquired through the keeping of his account")).

1. Virginia

To date, no Virginia court has recognized the tort for the breach of confidence within the context of a bank-client relationship; and the Court has no reason to think that the Supreme Court of Virginia would recognize such a tort under the facts of this case. *See M-CAM v. Richard D'Agostino*, 2005 U.S. Dist. LEXIS 45289, *5, 2005 WL 2123400 (W.D. Va. Sep. 1, 2005) ("Furthermore, there is no common law cause of action for such a breach of confidentiality under Virginia law."). The Plaintiffs have therefore failed to state a claim under Virginia law for the tort of breach of confidence. [21]

2. Florida

[21] The Court holds the same with respect to New York, Texas, and Washington. The Court is not aware of any decision under any of those states' law that has recognized a tort for the breach of confidence within the context of a bank/customer relationship. And in fact, New York courts have expressed reluctance to recognize such a tort. *See, e.g., Young v. United States Dep't of Justice*, 882 F.2d 633, 637 (2d Cir. 1989) (noting New York's reluctance to adopt the breach of confidence tort) (citing *Graney Development Corp. v. Taksen*, 92 Misc. 2d 764, 400 N.Y.S. 2d 717 (N.Y. Sup. 1978), *aff'd*, 66 A.D.2d 1008, 411 N.Y.S.2d 756 (N.Y. App. Div. 1978) (declining to adopt the tort).

Plaintiffs have asserted a plausible breach of confidence action under Florida law. In *Milohnihic v. First Nat'l Bank*, 224 So. 2d 759, 762 (Fla. Ct. App. 1969), a Florida Court of Appeals recognized an "implied duty on the part of a national bank not to disclose information negligently, willfully or maliciously or intentionally to third parties, concerning the depositor's account." In *Barnett Bank of West Florida v. Hooper*, 498 So. 2d 923, 925 (Fla. 1986), the Supreme Court of Florida concluded that a bank's implied duty to confidentiality to its depositors recognized in *Milohnihic* was not absolute; and that instead, a bank may, under certain circumstances, not be liable for disclosure provided the disclosure was pursuant to a public interest or competing public duty. *Id*. at 925-28.

Here, Plaintiffs allege that Capital One allowed a known vulnerability to persist on its systems which, left unresolved, effectively exposed the bank's customers' data to potential breach. That exposure was predicated on, at the least, a negligent act on the part of the Defendants not to remedy certain deficiencies. Neither Defendant asserts that there is a competing duty and/or public interest, as announced in *Barnett*, that justifies the information's disclosure. Therefore, the Court concludes that, under Florida law, the Plaintiffs have plausibly alleged a claim for breach of confidence.

3. California

California courts have specifically recognized the tort of breach of confidence. *Faris v. Enberg*, 97 Cal.App.3d 309, 158 Cal. Rptr. 704, 711 (Cal. App. Div. 1979). "This tort is based upon the concept of an implied obligation or contract between the parties that confidential information will not be disclosed." *Enter. Research Group, Inc. v. Genesis Creative Group, Inc.*, 122 F.3d 1211, 1226-27 (9th Cir.1997) (construing California law). "To prevail on a claim for breach of confidence under California law, a plaintiff must demonstrate that: (1) the plaintiff

conveyed 'confidential and novel information' to the defendant; (2) the defendant had knowledge that the information was being disclosed in confidence; (3) there was an understanding between the defendant and the plaintiff that the confidence be maintained; and (4) there was a disclosure or use in violation of the understanding." *Enter. Research Group*, 122 F.3d at 1227. Plaintiffs have alleged facts that make a breach of confidence claim plausible under California law.[22]

E. Breach of Contract

Plaintiffs allege Capital One breached a contract based on the alleged contracts formed by "fail[ing] to use reasonable measures to protect [plaintiff's] information." Am. Compl. ¶ 220.

In support of its breach of contract claim, Plaintiffs relies on Capital One's Privacy and Opt-Out Notice ("Privacy Notice"), wherein Capital One promised, under the heading "How does Capital One protect my personal information," that "[t]o protect your personal information from unauthorized access and use, we use security measures *that comply with federal law*. These measures include computer safeguards and secured files and buildings." *Id*. ¶¶ 98 & n.55, 217 (emphasis added). The Privacy Notice also lists the circumstances in which Capital One is permitted to disclose its customers' personal information to third parties, *id*. ¶¶ 217, which does not include the circumstances in which it was (involuntarily) disclosed here, *id*. ¶ 220.

Plaintiffs also allege Capital One breached promises in its Privacy Statement, in which Capital One represented to its customers that:

[22] Under California law, "there cannot be a valid, express contract and an implied contract, each embracing the same subject matter, existing at the same time." *Berkla v. Corel Corporation*, 302 F.3d 909, 917-18 (9th Cir. 2002) (citing *Fink v. Goodson-Todman Enters.*, 9 Cal.App.3d 996, 88 Cal. Rptr. 679, 690 (Cal. App. Div. 1970)). Plaintiffs have plausibly alleged a valid, express contract pertaining to the protection of Plaintiffs' PII, *see infra*; and their breach of confidence claim is based on an implied contract. Even though these claims are mutually exclusive, the Court will consider them to have been pled in the alternative, as permitted under Fed. R. Civ. P. 8(d)(2).

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices.

Id. ¶ 99. Capital One's website also represents, according to Plaintiff, that "security is a top priority," specifying that it "prohibit[s] the unlawful disclosure of [applicant's] Social Security number[s]" and that is uses "some of the strongest forms of encryption commercially available for use on the Web today." *Id*. ¶ 100. Together, these notices, Plaintiffs argue, ground a breach of contract claim against Capital One.

Capital One, in substance, contends that it did not assume a contractual obligation to use reasonable measures to protect Plaintiff's PII, and even if it had, Plaintiffs have not alleged any evidence that it breached that duty. More specifically, Capital One moves to dismiss on four grounds: (1) the Cardholder Agreements contain the only contractual terms between the parties.; (2) the Privacy Notice is not an enforceable agreement; (3) there was no "meeting of the minds" to make the Privacy Notice enforceable because Plaintiffs do not allege that they read, were aware of, or agreed to the terms of the Privacy Notice; and (4) its Privacy Notice does not contain enforceable promises, "only broad statements about corporate policy." [Doc. 387] at 33-35.

First, The Cardholder Agreement explicitly identify "privacy notices" as documents that "govern your Account with us," in addition to the Cardholder Agreement. *See* [Doc. 387], Exs. 2-10 p. 1 at "Account Documents". Thus, it would appear that the Cardholder Agreements do not contain all of Capital One's contractual commitments and the relationship between Plaintiffs and Capital One are subject to the privacy notices as well. *Second*, the same consideration that makes enforceable the Cardholder Agreements makes enforceable the Privacy Notices; and there is an objective manifestation of assent by both parties to enter into a contractual relationship based on

specific referenced terms, which included the privacy notices (and data security promises therein).[23] And *third*, the statements made in the Privacy Notices, construed in the light most favorable to plaintiffs, communicate a definite promise to maintain the security of Plaintiffs' information. Am. Compl. ¶ 98 (Capital One would protect the "personal information [the customers provide in order to obtain services] from unauthorized access and use [by employing] security measures that comply with federal law"); *Id.* ¶¶ 217(Capital One would disclose Plaintiffs' PII only in specifically authorized circumstances). *See also Marriott*, 440 F. Supp. 3d at 484-85 (concluding same under New York and Maryland law).

Finally, Plaintiffs have adequately alleged that by using inadequate data security measures that violated Section 5 of the FTC Act, related state statutes, and the GLBA's Safeguards Rule, Capital One breached the promise in the Privacy Notices to use security measures that comply with federal law, "internationally recognized security standards, regulations, and industry-based best practices," and "some of the strongest forms of encryption commercially available for use on the Web today," *id.* ¶¶ 99,100, 112. Against the background of the Data Breach, which occurred as the result of an alleged well-documented vulnerability in Capital One's platform, Plaintiffs have plausibly alleged that Capital One breached the obligations agreed to in its Privacy Notices. Therefore, Plaintiffs have sufficiently alleged a breach of contract under applicable Virginia law.

F. Unjust Enrichment

[23] In *Marriott*, the court applied the same contract principle to find Marriott's promises of adequate data security in its online privacy policies enforceable under Maryland and New York law, rejecting Marriott's similar argument that the plaintiffs were required to plead "they read, saw, or understood the Privacy Statements" to state a claim for breach of contract. 440 F. Supp. 3d at 484-85. The court concluded that the defendants' privacy statements "constitute objective offers to protect the personal information that it collects under the terms of the privacy statements." *Id.*

Plaintiffs also allege that both Capital One and Amazon were unjustly enriched by taking, retaining, and using Plaintiffs' PII for its own gain without expending sufficient resources to adequately protect that PII. Am. Compl. ¶¶ 181-195.

1. Capital One

The substantive law of unjust enrichment is largely consistent across each of the relevant jurisdictions. Broadly stated, the elements of an unjust enrichment claim are the receipt of a benefit and the unjust retention of the benefit at the expense of another. *See Peterson v. Cellco P'ship*, 164 Cal. App. 4th 1583, 1593, 80 Cal. Rptr. 3d 316 (Cal. Ct. App. 2008); *Fla. Power Corp. v. City of Winter Park*, 887 So. 2d 1237, 1241 n.4 (Fla. 2004); *Georgia Malone & Co. v. Ralph Rieder*, 86 A.D.3d 406, 411, 926 N.Y.S.2d 494 (N.Y. App. Div. 1st Dep't 2011) (same); *Heldenfels Bros., Inc. v. City of Corpus Christi*, 832 S.W.2d 39, 41 (Tex. 1992); *Schmidt v. Household Finance Corp.*, 276 Va. 108, 116, 661 S.E.2d 834 (Va. 2008); *Young v. Young*, 164 Wn.2d 477, 484, 191 P.3d 1258, 1262 (Wa. 2008); *see also* Restatement (First) of Restitution § 1 cmt. b (1937) ("A person confers a benefit upon another if he gives to the other possession of or some other interest in money, land, chattels, or choses in action, performs services beneficial to or at the request of the other, satisfies a debt or a duty of the other, or in any way adds to the other's security or advantage.").

There can be no recovery, however, under an unjust enrichment claim where there is an express contract between the parties covering the conduct at issue. There is no dispute that Plaintiffs have express contracts that govern their relationship with Capital One (*i.e.*, the Cardholder Agreements); and that express contract would ordinarily bar an unjust enrichment claim against Capital One. *See Diamond "S'' Dev. Corp. v. Mercantile Bank*, 989 So. 2d 696, 697 (Fla. Dist. Ct. App. 2008) (stating that an "unjust enrichment claim is precluded by the

existence of an express contract concerning the same subject matter"); *Clark-Fitzpatrick, Inc. v. Long Island R.R. Co.*, 70 N.Y.2d 382, 516 N.E.2d 190 (N.Y. 1987) (New York law) (same); *Coghlan v. Wellcraft Marine Corp.*, 240 F.3d 449, 454 (5th Cir. 2001) (Texas law) (same); *Lane Construction Co. v. Brown & Root, Inc.*, 29 F. Supp. 2d 707, 727 (E.D. Va. 1998), *rev'd in part on other grounds*, 207 F.3d 717 (4th Cir. 2000) (Virginia law) (same); *Goddard v. CSK Auto, Inc.*, 2013 Wash. App. LEXIS 2450, *20, 2013 WL 5638995 (Wash. App. Div. 1st Oct. 2014) (Washington law) (same). Here, however, there is a fundamental dispute between the parties concerning the scope of that contractual relationship and whether it definitively defines Capital One's obligations with respect to protecting Plaintiffs' PII. For that reason, the Court will treat Plaintiffs' unjust enrichment claim as an alternative claim to their express breach of contract claim; and for essentially the same reasons discussed below as to Amazon, Plaintiffs have plausibly alleged that if their express contractual relationship does not govern their rights with respect to the protection of their PII, they have stated a claim for unjust enrichment.

2. Amazon

There is no express contract between Plaintiffs and Amazon; and courts have concluded that the failure to secure a party's data can give rise to an unjust enrichment claim where a defendant accepts the benefits accompanying plaintiff's data and does so at the plaintiff's expense by not implementing adequate safeguards, thereby making it "inequitable and unconscionable" to permit defendant to retain the benefit of the data (and any benefits received therefrom), while leaving the plaintiff party to live with the consequences. *See, e.g.*, *Sackin*, 278 F. Supp. 3d at 751; *see also In re Target*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) ("If Plaintiffs can establish that they shopped at Target after Target knew or should have known of the breach, and that Plaintiffs would not have shopped at Target had they known about the

breach, a reasonable jury could conclude that the money Plaintiffs spent at Target is money to which Target 'in equity and good conscience' should not have received.").

Here, Plaintiffs have plausibly alleged that, in consideration for receiving credit services, Plaintiffs delivered to Capital One *and* Amazon their PII; had they known that Capital One and Amazon did not adequately protect that data, it would not have sought and purchased those services; and that Plaintiffs' purchase of Capital One's credit card services conferred a benefit on both Capital One and Amazon, by way of the fees and interest Plaintiffs' paid to Capital One and fees Capital One paid to Amazon for its use of AWS' servers. Am. Compl. ¶ 35 (noting that Amazon owns its server infrastructure which Capital One leased, paying for the computing power and storage it needs).

Amazon contends that Plaintiffs never conferred a benefit on it and that it had no knowledge of or access to Plaintiffs' PII on its servers. Both arguments, however, are plausibly refuted by the well-pled allegations in the Complaint. First, as alleged, Amazon (charging Capital One for server use) profited from its storage and retention of Plaintiffs' PII, uploaded to AWS via Plaintiffs' relationship with Capital One. Am. Compl. ¶¶ 183, 186, 195. Retaining these profits without adequately securing the data would be "unjust." Further, Amazon was well aware of Capital One's efforts to upload its customers' (and potential customers') PII to its servers. Indeed, to assuage customers of the very fear borne out by the Data Breach, Capital One and Amazon jointly developed Cloud Custodian in 2015 and 2016, in which Capital One "worked closely with the Amazon team" to develop a banking information security model that was better and more secure than Capital One's "own data centers." *Id.* ¶ 44; *see also id.* ¶¶ 90-91 ("At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the PII collected, maintained, and stored on the cloud is highly sensitive, susceptible to attack,

and could be used for malicious purposes by third parties . . . . Banking repositories and databases are popular and well-known targets for cyberattacks, especially given the extremely sensitive nature of the PII stored on those repositories and databases.").[24]

Based on these allegations, Court declines to dismiss Plaintiffs' unjust enrichment claim against Amazon as a matter of law.

G. Breach of Implied Contract

Plaintiffs allege that Capital One's act of taking possession of Plaintiffs' sensitive PII created an implied contractual obligation to provide adequate and reasonable data security. Am. Compl. ¶¶ 222-29. Plaintiffs further allege that Capital One breached this obligation by failing to maintain such measures to protect that information, and by disclosing that information to unauthorized third parties. *Id*. ¶ 228.

As with their unjust enrichment claim, an express contract precludes claims for actions covered by that contract based on implied contract. *See re Capital One Bank Credit Card Interest Rate Litig.*, 51 F. Supp. 3d 1316, 1351 (N.D. Ga. 2014) (applying Virginia law) ("To the extent that the Plaintiffs premise their implied contract or unjust enrichment theory on any actions covered by the 2005 Customer Agreement, the Court agrees that this claim would be barred under Virginia law by the existence of the written contract governing the parties' relationship"); *Marshall & Swift/Boeckh, LLC v. URS Corp.*, No. CV 08-4375-GAF, 2011 WL

[24] Nor is Amazon's lack of privity or direct relationship a bar to Plaintiffs' unjust enrichment claim. *See Metric Constructors, Inc. v. Bank of Tokyo-Mitsubishi, Limited*, 72 Fed. App'x 916, 923 (4th Cir. 2003) (recognizing unjust enrichment claim against third-party where "gravamen of Metric's unjust enrichment claim is that although the Banks were not parties to any contract with Metric, they nevertheless obtained a benefit from Metric's work on the project and that it would be unjust for the Banks to retain that benefit under the circumstances of this case."); *Alvardo v. Microsoft Corp.*, 2010 U.S. Dist. LEXIS 16437, at *10-15, 2010 WL 715455 (W.D. Wash. Feb. 22, 2010) (plaintiff could state a claim where licensing fees originally paid by plaintiff flowed through third party to defendant).

13174812, at *12 (C.D. Cal. Jan. 5, 2011) ("California law does not allow a party to bring an implied breach of contract or unjust enrichment claim when there exists an express agreement on point[.]"); *Clark-Fitzpatrick, Inc. v. Long Island R. Co.*, 516 N.E.2d 190, 193 (N.Y. 1987) ("The existence of a valid and enforceable written contract governing a particular subject matter ordinarily precludes recovery in quasi contract for events arising out of the same subject matter"); *Coghlan v. Wellcraft Marine Corp.*, 240 F.3d 449, 454 (5th Cir. 2001) (Texas law) ("In Texas, unjust enrichment is based on quasi-contract and is unavailable when a valid, express contract governing the subject matter of the dispute exists."); *Chandler v. Wash. Toll Bridge Authority*, 137 P.2d 97, 103 (Wash. 1943) ("A party to a valid express contract is bound by the provisions of that contract, and may not disregard the same and bring an action or an implied contract relating to the same matter, in contravention of the express contract," and applying principle to unjust enrichment claim).

Here, however, Defendants dispute that its obligation to secure and protect Plaintiffs' PII is within the scope of its express contract, the Cardholder Agreement, since the promises that Plaintiffs claim exist under their express contract, through the Privacy Notices, are, in fact, not part of their express contractual relationship. Accordingly, the Court will treat this implied contract claim as an alternative claim pursuant to Fed. R. Civ. P. 8(d)(2), to be pursued should it be determined that Capital One's obligations with respect to Plaintiffs' PII are not within the scope of their express contract.

H. Declaratory Judgment

Plaintiffs also allege a declaratory judgment claim against all Defendants. Capital One does not contest this claim, while Amazon does. Amazon contends that because Capital One addressed the vulnerabilities in its system and confirmed that there were no such further

instances "in its environment," Amazon Mot. at 29, there is no longer an ongoing controversy of "sufficient immediacy and reality to warrant the issuance of a declaratory judgment." [Doc. 464] at 19-20.

To state a claim for relief under the federal Declaratory Judgment Act, 28 U.S.C. § 2201, Plaintiffs must adequately allege a dispute that is: (1) "definite and concrete, touching the legal relations of parties having adverse legal interests"; (2) "real and substantial"; and (3) "admit[ting] of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." In that regard, "not . . . the brightest of lines" separates cases that satisfy the statutory jurisdictional requirements and those that do not. *MedImmune*, 549 U.S. 118, 127 (2007). The central question, however, is whether "'the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.'" *Id*. at 127 (quoting *Md. Cas. Co. v. Pac. Coal & Oil Co.*, 312 U.S. 270, (1941)).

Here, Plaintiffs have adequately alleged the existence of an actionable dispute for purposes of the Declaratory Judgment Act. Plaintiffs have plausibly alleged that there remains a dispute over the security of Plaintiff's PII, which continues to be stored on AWS's servers and remain subjected to a heightened risk of access and misuse by hackers. *See* Am. Compl. ¶ 17. Although Amazon contends that there can be no actionable dispute concerning the adequacy of its data security because Capital One disclosed that it had corrected the very vulnerability in its system, *see id*. ¶ 1, n.1, Plaintiffs have plausibly alleged the continued inadequacy of Defendants' security measures. And in that respect, Plaintiffs plausibly allege that they face a substantial risk of future harm if Amazon's security shortcomings are not redressed, making this

dispute sufficiently real and immediate with respect to the parties' legal relations, which are adverse. *See MedImmune*, 549 U.S. at 127. Likewise, this dispute underlying Plaintiffs' declaratory relief claim concerns Amazon's current security practices and their continued storage of Plaintiffs' PII, not a hypothetical set of acts or omissions regarding a speculatively likely data breach scenario. *See* Am. Compl. ¶¶ 17, 18-27, 36 (noting general risks involved with use of cloud storage), 58, 124 ("Without detailed disclosures to Capital One's customers, many class members are even to this day unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their PII without being able to take necessary precautions to prevent imminent harm."), 199.

Therefore, Plaintiffs have sufficiently alleged a declaratory relief claim, which, at this point, the Court will consider in its discretion.

I. Statutory Claims

Plaintiffs allege statutory claims under the laws of California, New York, Texas, Washington, and Virginia. Defendants move to dismiss each claim.

a. Virginia Data Breach Notification Law

The one Virginia Plaintiff, John Spacek, asserts a claim under the Virginia Data Breach Notification Law against Capital One and Amazon.

Virginia Code § 18.2-186.6(B) requires entities that possess the computerized data of a Virginia resident, including personal information, must disclose without unreasonable delay any breach of its security system upon discovery or notification of the breach. Notice must go to the Office of the Attorney General and any affected Virginia resident.[25]

[25] In full, the relevant statutory provision states:

> If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity

Capital One moves to dismiss this claim on four grounds: *First*, the Virginia law, according to Capital One, does not create a private right of action. *Second*, Plaintiff Spacek is not entitled to notice under the statute because he did not allege that his "personal information," as defined by statute, was compromised. *Third*, Capital One's "substitute notice," provided twelve days after it first became aware of the Cyber Incident, was timely as a matter of law. And *fourth*, Spacek has failed to allege that he suffered any damages unique to the timing (alleged delay) of Capital One's notification. At this stage of the litigation, none of these contentions warrant dismissal as a matter of law.

First, the statute expressly authorizes a Virginia resident to recover direct economic damages. While it is true that the statute authorizes the Attorney General to pursue such claims, the Attorney General does not have the exclusive right to do so. *See* Va. Code § 18.2-186.6 ("Except as provided by subsections J and K . . . [n]othing in this section shall limit an individual from recovering direct economic damages from a violation of this section."). Neither subsection J nor subsection K apply here.[26]

> reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law- enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law- enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

Va. Code § 18.2-186.6(B).

[26] Neither Capital One or Amazon contend that either subsection applies. Subsection J provides that "[a] violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator." Subsection K provides that "[n]othing

Second, Plaintiffs have adequately pled that Spacek's personal information, as defined in Va. Code § 18.2-186.6, was compromised. The statute defines "personal information" as "the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state *id*entification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number." Va. Code § 18.2-186.6(A). Here, the Complaint alleges that Capital One acknowledged that the stolen data included: *names*, addresses, zip codes, phone numbers, email addresses, dates of birth, self-reported income, *approximately 140,000 Social Security Numbers*, *80,000 bank account numbers*, credit scores, credit card limits, credit card balances, credit card payment history, and fragments of transaction data from 23 days during 2016, 2017, and 2018." Am. Compl. ¶ 2 & n.1 (emphasis added). Thus, it is plausibly alleged that the type of personal information allegedly compromised fits within the statutory definition.

Third, whether Capital One's substitute notice was timely is a question not ripe for the motion to dismiss stage. The notice's timeliness is a factual question that asks whether notice of the data breach occurred "without unreasonable delay." Va. Code § 18.2-186.6(B). Here, the Complaint alleges that it took Capital One approximately four (4) months to realize that there had been a breach, which, in fact, Capital One did not itself discover. Am. Compl. ¶¶ 125-126.

---

in this section shall apply to an individual or entity regulated by the State Corporation Commission's Bureau of Insurance." Va. Code § 18.2-186.6.

Moreover, the Complaint alleges that Capital One could have discovered the hack as early as April, since the hacker (Thompson) had posted her action on an online forum (Github). Further, there is no argument by Capital One that the law enforcement safe harbor, which permits a delay in notifying affected individuals, applies. In any event, these are all factual questions not suitable for disposition on a motion to dismiss.

And *finally*, Spacek has adequately alleged sufficient economic injury due to and traceable from the timing of the (delayed) notification. To be sure, there is an inference that Spacek suffered his alleged economic injuries *solely* a result of the data breach itself. Nevertheless, had Spacek been aware of the breach earlier, it is also plausible that there were incremental, additional economic injuries beyond those arising from the Data Breach, namely additional monitoring costs that Spacek would not have otherwise taken, which are traceable to Capital One's delay. Whether these incremental, additional costs are different from Spacek's injuries arising from the data breach itself is, at this stage, unknown. Equally unknown is whether Spacek would not have engaged in these behaviors even if he were timely notified. However, construing the allegations in the light most favorable to Plaintiff Spacek, the economic harm alleged plausibly falls within the scope of the statute. *See* Va. Code § 18.2-186.6(I) ("Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.").[27]

[27] No Virginia court has interpreted what constitutes "direct economic damages." One California court has, but dismissed the Virginia claim on the grounds that the Virginia plaintiff had failed to assert any cognizable damages specific to the failure to notify him of the data breach, since the cognizable injury (expense associated with monitoring account from fraud) arose only from the data breach itself. *See Corona v. Sony Pictures Entm't, Inc*., 2015 U.S. Dist. LEXIS 85865, at *11, 2015 WL 3916744 (C.D. Cal. 2015). Plaintiff Spacek is distinguishable from the *Corona* plaintiff because he has actually alleged identity theft and unauthorized charges *after* the Data Breach. Am. Compl. ¶ 26.

This conclusion also applies to Amazon. The only issue with respect to Amazon is whether Amazon, like Capital One, had an obligation to disclose the Data Breach. In that regard, the Virginia statute imposes an obligation to "an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license . . . ." And as pled, the Complaint alleges that Amazon, on whose server the Plaintiffs' information was stored, is an entity that own[s], license[s], or maintain[s] computerized data that includes Personal Information as defined by Va. Code §§ 18.2-186.6(B), (D). Although no Virginia court has yet to extend this statute to a third-party provider like Amazon, given the statute's plain language—particularly, the statute's application to any entity that "maintain[s] computerized data"—the Amended Complaint has adequately alleged that Amazon falls within the scope of the Virginia Data Breach Notification Law. *See* Am. Compl. ¶¶ 35, 88, 120

b. Washington Data Breach Notification Statute

For the same reasons discussed with respect to Virginia's Data Breach Notification Statute, the Washington Plaintiffs' claims under the Washington Data Breach Notification Statute also survives the Motions.

Amazon contends that because it is not an owner of Plaintiffs' data, it did not need to notify Plaintiffs. To be sure, the Amended Complaint does not allege that Amazon actually "owns" Plaintiff's personal information. That said, the Washington state statute still imposes an obligation on Amazon to notify the consumer of a data breach over any information it "maintains." *See* Wash. Rev. Code. ("RCW") 19.255.10(2) ("Any person or business that *maintains* data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to

have been, acquired by an unauthorized person.") (emphasis added); RCW 19.255.(13)(a) ("Any consumer injured by a violation of this section may institute a civil action to recover damages."). Because Amazon, on whose servers Capital One's data was held, plausibly maintained the data, *see* Am. Compl. ¶¶ 35, 88 (At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the PII collected, *maintained*, and stored on the cloud is highly sensitive, susceptible to attack. . .") (emphasis added), 120, the Court finds that Amazon is plausibly liable under the Washington State Data Breach Notification Statute.

c. California Unfair Competition Law

The California Plaintiffs, individually and on behalf of the California subclass, assert violations under the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq.* 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 Defendants violated the UCL by: (1) failing to implement and maintain reasonable security measures to protect their personal information; (2) 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; and (3) 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. Am. Compl. ¶¶ 233-235.

Defendants move to dismiss this claim, arguing that (1) Plaintiffs have failed to allege a cognizable injury and thus lack standing to assert the claim; (2) cannot rely on omissions as a basis to allege a violation under the UCL; (3) have failed to allege fraud, as is necessary, with particularity, as required by Federal Rule of Civil Procedure 9(b); and (4) have failed to satisfy UCL's unlawfulness prong. None of these arguments is availing.

First, the California Plaintiffs have sufficiently alleged UCL standing. To assert standing under the UCL, a party must show that it is a "'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 this regard, a person "must demonstrate some form of economic injury," which, as the *Kwikset* court held, can be shown where a plaintiff "surrender[s] in a transaction more, or acquires in a transaction less, than he or she otherwise would have . . . ." 246 P.3d at 885-86. *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 U.S. Dist. LEXIS 42696, 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, the California Plaintiffs have alleged that "had consumers known the truth about Defendants' data security practices, they would not have purchased Capital One's product, and/or would have paid less." Am. Compl. ¶ 275. This is sufficient to establish standing for the

UCL claim. *See Kwikset*, 246 P.3d at 885-86; *accord In re Marriott Int'l, Inc.*, 2020 U.S. Dist. LEXIS 30435, at *145-46.

Moreover, California Plaintiff Tada claims she spent money purchasing credit-monitoring and identity-theft services to mitigate the damages related to the Data Breach, which remain unreimbursed. Am. Compl. ¶¶ 25, 27. Thus, unlike certain California cases which have declined to recognize UCL standing where a plaintiff had been reimbursed for economic damages incurred, *see, e.g.*, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 U.S. Dist. LEXIS 152838, 2016 WL 6523428, at *11 (S.D. Cal. Nov. 3, 2016); *Ruiz v. Gap, Inc.*, 2009 U.S. Dist. LEXIS 10400, 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 had offered credit monitoring services), *aff'd*, 380 F. App'x 689 (9th Cir. 2010), the pleadings here do not indicate that any of Tada's expenses arising from the Data Breach have been reimbursed. Therefore, these payments also constitute economic injury, sufficient to confer UCL standing. *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").[28]

[28] The Court notes that "[a]lthough the requirements of federal standing under Article III and the requirements of standing under California's consumer protection statutes overlap, there are important differences." *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 965 (S.D. Cal. 2012) (citing *Troyk v. Farmers Grp., Inc.*, 171 Cal. App. 4th 1305, 90 Cal. Rptr. 3d 589, 625 n.31 (Ct. App. 2009)). "For example, under Article III, a plaintiff must allege: (1) an injury in fact; (2) causation; and (3) likelihood that the injury will be redressed by a favorable decision." *Id.* Meanwhile, for purposes of the UCL, a plaintiff need meet only "the first element (i.e., an injury in fact)," which requires some showing that a party lost actual money or property. *Id.* (internal quotation marks omitted); *see also Ehret v. Uber Technologies, Inc.*, 68 F. Supp. 3d 1121, 1132 (N.D. Cal. 2014) ("Whereas a federal plaintiff's injury in fact may be intangible and need not involve lost money or

Second, the California Plaintiffs have alleged, with the requisite level of detail and particularity, the "who" (Capital One and Amazon); the "what" (Capital One and Amazon retained and stored Plaintiffs' data in an insecure manner and made affirmative misrepresentations and material omissions regarding the adequacy of that security); and the "when and where" (the deficient data security policies and representations were in place prior to the data breach). They also allege that Amazon knew of its servers' vulnerability to attacks, Am. Compl. ¶¶ 46, 53-54; Amazon and Capital One jointly announced that they had developed a software, Cloud Custodian, to solve the security problems posed by Amazon's data security services, *id*. ¶¶ 56, 58; Cloud Custodian did not actually resolve the issue; and despite this, Capital One nevertheless proceeded to use Amazon's vulnerable servers while simultaneously affirming the success of its Cloud Custodian software and commitment to data security, which induced customers to look to Capital One, *id*. ¶ 59. "In short, the Complaint contains extensive allegations that [Capital One and Amazon] 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." *In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at 491.

Finally, the California Plaintiffs' allegations—as it pertains to both Amazon and Capital One—satisfy the UCL's unlawfulness prong. The unlawfulness prong of the UCL "borrows violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable." *Cal. Consumer Health Care Council v. Kaiser Found. Health Plan, Inc.*, 142 Cal. App. 4th 21, 27 (2006) (internal quotations omitted). Thus, in determining

---

property, . . . a UCL plaintiff's injury in fact [must] specifically involve lost money or property.") (internal quotation marks omitted).

whether the unlawfulness prong has been met, the court must "look through" the asserted UCL claim and determine if the underlying statutes cited state a claim for relief. *Id*. at 28 (affirming dismissal of the UCL claim after in-depth analysis of the underlying statute and concluding, "[w]e find nothing in the language of this particular provision to support appellant's interpretation of it."). Accordingly, the California Plaintiffs "must identify the particular section of the statute that was violated, and must describe with reasonable particularity the facts supporting the violation." *Brothers v. Hewlett-Packard Co.*, 2006 U.S. Dist. LEXIS 82027, 2006 WL 3093685, at *7 (N.D. Cal. Oct. 31, 2006) (applying *Khoury v. Maly's of California, Inc.*, 14 Cal. App. 4th 612, 619, 17 Cal. Rptr. 2d 708 (1993)).

To satisfy this prong, the California Plaintiffs allege that Defendants violated, among other statutes, Section 5 of the FTC Act. *See In re Anthem Data Breach Litig.*, 162 F. Supp. 3d 953, 989, 2016 U.S. Dist. LEXIS 18135, *154 (holding Complaint sufficiently alleged allegations of unlawfulness prong). As discussed above, Section 5 of the FTC Act applies here and provides an ascertainable duty regarding data protection. *See In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at . Therefore, Plaintiffs have adequately alleged the unlawfulness prong of an UCL claim.

d. California, Florida, New York, Texas and Washington State Consumer Protection Statutes

Plaintiffs bring consumer protection claims under the laws of California, New York, Texas, and Washington. Defendants move to dismiss each of these claims.

i. California

The California Plaintiffs allege a claim under California Consumer Legal Remedies Act ("CLRA"), Cal Civ. Code §§ 1750, *et seq.*, individually and on behalf of the California subclass. Compl. ¶¶ 240-251. Defendants moves to dismiss this claim on four grounds. *First*, Plaintiffs

have failed to allege a cognizable injury. *Second*, Plaintiffs have failed to state a requisite consumer transaction, as required under the CLRA. *Third*, Plaintiffs' liability cannot be based on alleged omissions, as there is no duty to disclose. And *fourth*, Defendants argue that Plaintiffs have failed to plead their claims with sufficiently particularity to meet the requirements of Rule 9(b).

Under the CLRA, a plaintiff may bring a claim when "any person" uses a statutorily prohibited trade practice "in a transaction . . . which results in the sale or lease of goods or services to any consumer." Cal. Civ. Code § 1770. As stated in the statute itself, the CLRA "shall be liberally construed and applied to promote its underlying purposes, which are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection." *Id*. at § 1760.

As an initial matter, Defendants argue that because loan or extensions of credit at issue here are not "goods" or "services," as defined under the CLRA, Plaintiffs' claims fall outside the ambit of the CLRA. The CLRA applies only to a limited set of consumer transactions; and it is not a law of "general applicability." In that regard, a "consumer," the object of the CLRA, is defined as "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." Cal. Civ. Code § 1761(d). "Goods" is defined as "tangible chattels bought or leased for use primarily for personal, family, or household purposes." *Id*. § 1761(a). And "services" is defined as "work, labor, and services for other than a commercial or business use including services furnished in connection with the sale or repair of goods. " *Id*. § 1761(b). The issue here reduces to whether Plaintiffs entered into a consumer transaction involving either "goods" or "services" with Capital One and Amazon.

Notably, the CLRA does not expressly list "loans" or "credit" as a form of good or service, and the legislative history suggests that the California Assembly did not intend to include loans or credit, standing alone, within the scope of the CLRA. *See Berry v. Am. Express Publ'g, Inc.*, 54 Cal. Rptr. 3d 91, 97 (Cal. App. 2007). Indeed, early, but later rejected, drafts of the CLRA defined "consumer" as "an individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes." *See* Assem. Bill No. 292 (1970 Reg. Sess.) Jan. 21, 1970 (emphasis added). California courts have viewed the California legislature's decision to remove credit transactions as persuasive evidence that any credit transactions of the type here do not fall within the CLRA's coverage. *See Berry*, 54 Cal. Rptr. at 91 (finding that neither the express text of CLRA nor its legislative history supports the notion that credit transactions separate and apart from any sale or lease of goods or services are covered under the [CLRA]."); *see also Wilson v. City of Laguna Beach*, 6 Cal. App. 4th 543, 555, 7 Cal. Rptr. 2d 848 (Cal. App. 1992) ("The rejection by the Legislature of a specific provision contained in an act as originally introduced is most persuasive to the conclusion that the act should not be construed to include the omitted provision.").

But California courts have also recognized that *Berry* did not entirely preclude the application of the CLRA to certain consumer transactions and have consistently allowed cases involving credit and other financial transactions to proceed past the motion to dismiss stage provided other ancillary or tangential "services" related to a financial transaction exist. *See, e.g.*, *Hernandez v. Hilltop Fin. Mortg., Inc.*, 622 F. Supp. 2d 842, 850-51 (N.D. Cal. 2007); *Jefferson v. Chase Home Finance LLC*, 2007 U.S. Dist. LEXIS 36298, 2007 WL 1302984, at *3 (N.D. Cal. May 3, 2007) (concluding that the loan transaction between a mortgage finance company and the plaintiff involved "more than the provision of a loan; they also include [the] financial

services [of managing the loan]."); *Corbett v. Hayward Dodge, Inc.*, 119 Cal. App. 4th 915, 14 Cal. Rptr. 3d 741 (Cal. App. 2004) (automobile loans); *Kagan v. Gibraltar Savings and Loan Ass'n*, 35 Cal.3d 582, 200 Cal. Rptr. 38, 676 P.2d 1060 (Cal. 1984) (Individual Retirement Accounts); *Knox v. Ameriquest Mortgage Co.*, 2005 U.S. Dist. LEXIS 40709, 2005 WL 1910927, at *4 (N.D. Cal. Aug. 10, 2005) (finding that, in the context of predatory lending allegations, "California courts generally find financial transactions to be subject to the CLRA."); *In re Ameriquest Mortgage Co.*, No 05-CV-7097, 2007 U.S. Dist. LEXIS 29643, 2007 WL 1202544, at *6 (N.D. III. Apr. 23, 2007) (stating, in the credit card context, that the "cards provide a certain 'convenience service:' users may not need to carry large amounts of cash; they may gain favorable credit ratings through using the cards; and they may be able to buy expensive items without going through the time-consuming process of securing a personal loan"). As explained in *Hitz v. First Interstate Bank*, 38 Cal. App. 4th 274, 44 Cal. Rptr. 2d 890 (Cal. App. 1995) (non-CLRA context), a credit product or transaction may provide some independent service susceptible to CLRA coverage. Thus, while the credit feature of a credit card, standing alone, is likely not covered by the CLRA, credit cards provide more value to a consumer than just the credit line they represent; and credit products can fall within the CLRA's ambit. *Id*. at 286-87.

Here, as alleged, it is plausible that the sort of services that California courts have recognized as "services" within the meaning of § 1761(b) exist. Not only did Plaintiffs seek a loan, but, upon receiving such a line of credit, they ostensibly received the services in developing, securing, maintaining that credit line; and they sought benefits associated with the use of the credit card. Therefore, based on the facts alleged, Plaintiffs have plausibly alleged the

existence of tangential services, besides an extension of credit or a financial transaction, that establishes its transactions with Capital One were covered by the CLRA.[29, 30]

ii. Florida[31]

The Florida Plaintiffs, individually and on behalf of the Florida subclass, allege a claim under the Florida Deceptive and Unfair Trade Practice Act ("FDUTPA"), Fla. Stat. §§ 501.201-510.213.

The FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce . . . ."

---

[29] As discussed above, Plaintiffs have alleged, with particularity, the alleged deceptive acts that adequately satisfy Rule 9(b). Moreover, contrary to Defendants' suggestion otherwise, an omission, as opposed to an affirmative misrepresentation, can ground a claim under the CLRA. *See In re Adobe Sys. Inc. Privacy Litig*, 66 F. Supp. 3d 1197, 1229 (N.D. Cal. 2014).

[30] Plaintiffs have not, as a matter of law, asserted a cognizable CLRA claim against Amazon. The CLRA provides that "[t]hirty days or more prior to the commencement of an action for damages pursuant to this title, the consumer shall [in writing and sent by certified or registered mail, return receipt requested, to the place where the transaction occurred or to the person's principal place of business within California] do the following: (1) Notify the person alleged to have employed or committed methods, acts, or practices declared unlawful by Section 1770 of the particular alleged violations of Section 1770. (2) Demand that the person correct, repair, replace, or otherwise rectify the goods or services alleged to be in violation of Section 1770." Cal. Civ. Code § 1782. The purpose of the CLRA's notice requirement is "to provide and facilitate pre-complaint settlements of consumer actions wherever possible and to establish a limited period during which such settlement may be accomplished." *Outboard Marine Corp. v. Super. Ct.*, 52 Cal. App. 3d 30, 41, 124 Cal. Rptr. 852 (1975). Courts require strict compliance with the notice requirement. *Allen v. Similasan Corp.*, 2013 U.S. Dist. LEXIS 139874, 2013 WL 5436648, at *2-3 (S.D. Cal. Sept. 27, 2013). Here, Plaintiffs did not attach the required pre-suit notices to the Amended Complaint. And the only two pre-suit notices Plaintiffs have provided, *see* [Doc. 426], Exs. A-C, both fail to abide by the terms of § 1782. Plaintiff Michele Desoer submitted a notice on August 6, 2019, with a return receipt dated August 8, 2019, three days *after* filing her action on August 5, 2019. *See* No. 2:19-cv-01223-MLP (W.D. Wa. Aug. 5, 2019). Likewise, Plaintiffs Ursula Riley, Howard Chen, and Jarod Thrush appear to have submitted a notice to Amazon on August 26, 2019, three days *before* they filed their action on August 29, 2019. *See* No. 2:19-cv-01366-BAT (W.D. Wa. Aug. 26, 2019)*; see also Von Grabe v. Sprint PCS*, 312 F. Supp. 2d 1285, 1304 (S.D. Cal. 2003) (dismissing CLRA claim with prejudice due to plaintiff's failure to provide statutory notice).

[31] Plaintiffs "do not dispute that they do not state a claim against Capital One for violation of the Florida Deceptive and Unfair Trade Practices Act." [Doc. 427] at 43. Therefore, the Court dismisses the claim (only as against Capital One) as abandoned.

Fla. Stat. § 501.204(1); *see also Baptist Hosp., Inc. v. Baker*, 84 So. 3d 1200, 1204 (Fla. 1st DCA 2012) (noting FDUTPA protects both the consuming public and legitimate business enterprises from such practices). The FDUTPA is to be "construed liberally to promote" the policy of "protect[ing] the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2). Thus, as with the other consumer protection claims discussed *infra*, to bring a FDUTPA claim for damages, a plaintiff must establish: (1) a deceptive act or unfair practice; (2) causation; and (3) actual damages. *Baptist Hosp.*, 84 So. 3d at 1204. In moving to dismiss this claim, Amazon argues that the Florida Plaintiffs have failed to dispute the lack of causation and damages.[32] [Doc. 464] at 18.

The FDUTPA does not require that a plaintiff prove the consumer actually relied on the deceptive or unfair practice. *See Cold Stone Creamery, Inc. v. Lenora Foods I, LLC*, 332 F. App'x 565, 567 (11th Cir. 2009); *see also Davis v. Powertel, Inc.*, 776 So. 2d 971, 973 (Fla. 1st DCA 2000) ("A party asserting a deceptive trade practice claim need not show actual reliance on the representation or omission at issue."); *State, Office of Attorney Gen., Dep't of Legal Affairs v.*

[32] In *Burrows v. Purchasing Powers, LLC*, 2012 U.S. Dist. LEXIS 186556 (S.D. Fla. Oct. 18, 2012), the district court denied the defendant's effort to dismiss plaintiff's FDUTPA claim. There, the court found that the plaintiff had adequately alleged an unfair practice, as defined under the FDUTPA, because the material misrepresentations made by the defendant regarding the adequacy and measures undertaken to protect plaintiff's PII caused, or were likely to cause, substantial injury to consumers, not reasonably avoidable by the consumers themselves, and certainly not outweighed by any countervailing benefits enjoyed by the plaintiffs. See *id*., at *18 (defining "unfair practice" as "one that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'") (quoting I*n re Motions to Certify Classes Against Court Reporting Firms for Charges Relating to World Indices*, 715 F. Supp. 2d 1265, 1277 (S.D. Fla. 2010). Thus, because Amazon, as alleged, made similar representations regarding the adequacy of its data security hosted on its AWS servers, which, as alleged, have caused substantial injury to Plaintiffs not otherwise avoidable, the Florida Plaintiffs have alleged a cognizable unfair practice, an element to the Florida Plaintiffs' FDUTPA claim.

Commerce Commercial Leasing, LLC, 946 So. 2d 1253, 1258 (Fla. 1st DCA 2007) ("A deceptive or unfair trade practice constitutes a somewhat unique tortious act because, although it is similar to a claim of fraud, it is different in that, unlike fraud, a party asserting a deceptive trade practice claim need not show actual reliance on the representation or omission at issue." (internal quotation omitted)). Instead, a plaintiff need only provide that "the alleged practice was likely to deceive a consumer acting reasonably in the same circumstances." *Cold Stone*, 332 F. App'x at 567.

Here, the Florida Plaintiffs alleges that Amazon's misrepresentations concerned the privacy and confidentiality of the Florida subclass's PII, including implementing and maintaining reasonable security measures and misrepresentation that they would comply with common law and statutory duties, omitting and suppressing and concealing the material fact that they did not reasonably or adequately secure the Florida Plaintiffs' PII. Am. Compl. ¶ 255. Plaintiff further alleges that these representations and omissions "were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII." *Id.* ¶ 256. Although expressed in general terms, the Florida Plaintiffs sufficiently allege that Amazon's misrepresentations are "likely to deceive a consumer acting reasonably in the same circumstances. *Cold Stone*, 332 F. App'x at 567. Therefore, the Florida Plaintiffs have alleged causation.

Separately, under the FDUTPA, a party may recover actual damages, measured by "the difference in the market value of the product or service in the condition in which it was delivered and its market value in the condition in which it should have been delivered according to the contract of the parties." *Rollins, Inc. v. Heller*, 454 So. 2d 580, 585 (Fla. 3d DCA 1984) (describing this measurement as being "well-defined in the case law"). Here, the Florida

Plaintiffs assert that Amazon's unfair and deceptive acts and practices caused "ascertainable losses of money or property . . . including loss of the benefit of their bargain with and overcharges by Capital One, [since] they would not have paid Capital One for their services or would have paid less for such services but for the [deceptive and unfair acts] alleged [in the Complaint]." Am. Compl. ¶ 258. Because the Florida Plaintiffs have sufficiently alleged that the misrepresentations and omissions made by Amazon affected the value of the credit product they purchased, the Florida Plaintiffs have asserted a cognizable form of damages sufficient to support their FDUTPA claim.[33]

iii. New York

The New York Plaintiffs, individually and on behalf of the New York subclass, allege a claim under the New York General Business Law ("GBL"), N.Y. Gen. Bus. §§ 349, *et seq.* *See* Am. Compl. ¶¶ 260-67. Defendants move to dismiss this claim, arguing that the New York Plaintiffs have failed to allege a cognizable injury or plead their claims with sufficiently particularity to meet the requirements of Rule 9(b). Neither argument is availing.

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 claim under § 349(a), 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

[33] Florida courts have been clear, however, that consequential damages cannot sustain a FDUTPA claim. *See, e.g.*, *BPI Sports, LLC v. Labdoor, Inc.*, 2016 U.S. Dist. LEXIS 23033, at *17 (S.D. Fla. Feb. 25, 2016) (collecting cases) (dismissing FDUTPA claim because "[plaintiff] does not present any facts supporting a claim that [defendant's] study has affected the market value of [plaintiff's] product," instead relying on a consequential damages theory (lost profits and business) that is not cognizable under the FDUTPA). For example, such consequential damages from the Data Breach would include the costs for credit monitoring and identity protection services or the time and expenses related to monitoring their financial accounts since they bear no relation to the diminution in the product value.

plaintiff "suffered injury as a result of the deceptive act." *Stutman v. Chem. Bank*, 95 N.Y.2d 24, 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*, 98 N.Y.2d 314, 774 N.E.2d 1190, 1195 (N.Y. 2002).

Each of the New York Plaintiffs allege that he or she "is a resident of New York" and "applied for and used [his and her] Capital One credit card in New York, and provided [his and her] PII to Capital One in order to do so." Am. Compl. ¶¶ 22-23. The New York Plaintiffs further allege that, "as a result of the Data Breach," they spent time and effort to regularly monitor the accounts to detect fraudulent activity to mitigate potential harm and, in the case of Plaintiff Gershen, spent significant time to "resolve the unauthorized efforts to explore her PII and to protect against further attacks on her credit, including placing freezes on her credit reports and spending money hours ensuring there were no further authorized charges or accounts and that the fraudulent accounts were closed." *Id.* In this regard, the New York Plaintiffs allege that Defendants' 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 remediate identified security and privacy risks, failing to comply with statutory duties regarding the security and privacy of their personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, misrepresenting and omitting that it would protect the Plaintiffs' personal information, and misrepresenting and omitting that it would comply with common law and statutory duties pertaining to data security. Am. Compl. ¶¶ 259-261. Moreover, Plaintiffs claim that these acts affected the public interest and consumers at large, resulting in damages. *Id.* ¶ 265.

First, unlike the UCL, "an action under [GBL] § 349 is not subject to the pleading-with-particularity requirements of Rule 9(b)." Instead, it "need only meet the bare-bones notice-pleading requirements of Rule 8(a)." *Pelman ex rel. Pelman v. McDonald's Corp*, 396 F.3d 508, 511 (2d Cir. 2005) (citation omitted); *see also id.* ("[B]ecause § 349 extends well beyond common-law fraud to cover a broad range of deceptive practices, . . . a private action under § 349 does not require proof of the same essential elements (such as reliance) as common-law fraud."). As the Court has already explained, Plaintiffs have adequately alleged that Defendants made various and specific representation that the New York Plaintiffs' PII would be protected, including representations made on Defendants' websites and in the Privacy Notices. Thus, the Court finds that the New York Plaintiffs have sufficiently alleged their claims under Rule 8. *See also In re Anthem Data Breach Litig.*, 162 F. Supp. 3d at 996 (finding same).[34]

Second, Plaintiffs allegations state a cognizable injury. Parties seeking damages under the GBL must provide "proof that a material deceptive act or practice caused actual, although not necessarily pecuniary, harm." *Small v. Lorillard Tobacco Co., Inc.*, 94 N.Y.2d 43, 720 N.E.2d 892, 897, 698 N.Y.S.2d 615 (N.Y. 1999) (internal quotation marks and emphasis omitted). For purposes of this definition, Plaintiffs allegations that they would not have entered into a transaction with Capital One had they known about the inadequate data security is a cognizable, and thus sufficient, ground for damages. In *Orlander v. Staples, Inc.*, 802 F.3d 289, 301 (2d Cir. 2015), the Second Circuit held that plaintiff, who pled that "he would not have purchased [a set of services] had he known that [d]efendant intended to decline to provide him any [such]

[34] And even if Plaintiffs were required to meet Rule 9(b)'s pleading requirements, as discussed above with respect to their UCL claims, Plaintiffs similar, if not identical allegations, alleged with respect to the GBL claim meet the requirements of Rule 9(b).

services" during the first of year of his contract, "sufficiently alleged an injury stemming from [a] misleading practice" under the GBL. The same is true here. Plaintiffs allege that, "if [plaintiffs] had known that Capital One's data security measures were inadequate to safeguard customers' PII from theft, [they] would not have applied for or used Capital One credit cards or provided her PII." Am. Compl. ¶¶ 22-23.

Accordingly, for these reasons, the New York Plaintiffs have sufficiently pled injury under GBL § 349 and their GBL claim may proceed.

iv. Texas

Texas Plaintiff Whitney Anne Palencia, individually and on behalf of the Texas subclass, alleges a claim under the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), Texas Bus. & Com. Code §§ 17.41, *et seq.*

The DTPA grants "consumers" a cause of action for false, misleading, or deceptive acts or practices. Tex. Bus.& Com. Code § 17.50(a)(1). To raise a claim under the DTPA, the plaintiff must be a "consumer." *Mendoza v. American Nat'l Ins. Co.*, 932 S.W.2d 605, 608 (Tex. App.-San Antonio 1996) (a plaintiff must qualify as a "consumer" in order to have standing under the DTPA). In relevant part, the DTPA defines a "consumer" as "an individual . . . who seeks or acquires by purchase or lease, any goods or services." Tex. Bus. & Com. Code § 17.45(4). Under the DTPA, whether a party is a "consumer" is a question of law. *Grant-Brooks v. WMC Mortgage Corp.*, 2003 U.S. Dist. LEXIS 22593, 2003 WL 23119157 *7 (N.D. Tex. 2003).

In moving to dismiss this claim, Defendants, citing *Marketic v. U. S. Bank Nat'l Ass'n*, 436 F. Supp. 2d 842, 854 (N.D. Tex. June 15, 2006), argue that the Texas Plaintiff is not a "consumer" under the DTPA. [Doc. 387] at 44. In *Marketic*, the federal district court found that

because the purchase of intangible property rights—in *Marketic*, a home equity loan—is generally not considered a purchase of goods or services, the plaintiff could not show that she was a "consumer" under the DTPA. *Id.*; *see also Grant-Brooks v. WMC Mortg. Corp.*, 2004 U.S. Dist. LEXIS 22593, 2004 WL 1194462 *5 (N.D. Tex. 2004) (holding same). Relying on *Marketic* and noting that the allegations in the Complaint are only that Plaintiffs applied for and used a Capital One credit card, *see* Am. Compl. ¶ 24, Defendants contend that no Texas subclass member can qualify as a "consumer."

In *Riverside Nat'l Bank v. Lewis*, 603 S.W.2d 169 (Tex. 1980), the Supreme Court of Texas held that borrowing money is not seeking or acquiring any services and therefore cannot form the basis of a consumer transaction. In particular, the *Riverside* court clarified that because "money is not . . . a 'good'" and because "the DTPA's use of the word 'services' d[oes] not include the extension of credit, or the borrowing of money," a claimant who sought only to borrow money cannot qualify as a "consumer" under the DTPA. *Riverside Nat'l Bank*, 603 S.W.2d at 175 (any "attempt to acquire money, or the use of money, [i] s not an attempt to acquire services"). Because *Riverside* appears to foreclose the creation of a "consumer" relationship predicated on a financial transaction of the type here, Plaintiff Palencia is arguably not a "consumer." On the other hand, the Supreme Court of Texas, interpreting the DTPA, has elsewhere stated that bank customers do not, in every instance, fail to qualify as a "consumer." In *Knight v. Int'l Harvester Credit Corp.*, 627 S.W.2d 382 (Tex. 1982) and *Flenniken v. Longview Bank & Trust Co.*, 661 S.W.2d 705 (Tex. 1983), the Supreme Court of Texas found that a bank customer qualified as a "consumer" because, in each case, the plaintiff sought financing or became a bank customer because, or in search of, financing to purchase a consumer good—in *Knight*, a dump truck and in *Flenniken*, a house.

Here, Plaintiff Palencia alleges that she was "approved for and issued a Capital One credit card in 2018 and used the card for several months before paying off the balance on and discontinuing use of the card in October 2018." Am. Compl. ¶ 24. While there are no specific allegations, similar to those found *Knight* or *Flenniken*, that Plaintiff specifically sought the credit card services received from Capital One to seek or acquire certain "goods" or "services" of the type discussed in *Knight* or *Flenniken*, read in a light most favorable to her, Plaintiff Palencia's allegations raise the plausible inference that, in receiving a credit line from Capital One, she sought to acquire good and services, as required by Tex. Bus. & Com. Code § 17.45(4) for "consumer" status.[35] Therefore, Plaintiff Palencia meets the DTPA's test for "consumer" and has standing to bring this action.

Defendants further argue that Plaintiff Palencia has not successfully stated a claim under the DTPA because she cannot ground her claim in a duty to disclose and that liability cannot be based on an alleged omission. [Doc. 387] at 44-45. But the DTPA itself provides that omissions are independently actionable, *see* Tex. Bus. & Com. Code § 17.46(b)(24) ("the term 'false, misleading, or deceptive acts or practices" includes . . . (24) failing to disclose information

[35] In this regard, the allegations here are distinguishable from those found in *Cushman v. GC Servs., LP*, 657 F. Supp. 2d 834, 843 (S.D. Tex. 2009). In *Cushman*, the plaintiff filed an action seeking damages arising from certain debt collection practices in connection with a debt owed on her American Express credit card. There, the plaintiff alleged that the defendant debt collector's practices violated, *inter alia*, the DTPA. In support of that claim, Plaintiff argued that Defendant had made certain material misrepresentations, which it knew or should have known to be false. 657 F. Supp. 2d at 837. In finding that the plaintiff did not qualify as a "consumer," the Texas federal court noted that its was bound by "the Texas Supreme Court's holding that an "attempt to acquire money, or the use of money, [i]s not an attempt to acquire services and money is not a good." *Id*. at 844 (internal quotations omitted). The court went on to hold that because plaintiff had not alleged the she had sought to acquire goods or services by use of her credit card, she could not qualify as a consumer. *Id*. Here, in contrast, the reasonable inference to be drawn in favor of Plaintiff Palencia is that she opened and used her credit line for the purpose of purchasing goods and services.

concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed"), and Texas case law recognizes that once a party decides to voluntary disclose information on the subject, a duty to disclose information not otherwise available to the consumer and within the seller's knowledge exists, *see Four Bros. Boat Works, Inc. v. Tesoro Petroleum Cos.*, 217 S.W.3d 653, 670 (Tex. App. 2006); *cf. Chandler v. Gene Messer Ford, Inc.*, 81 S.W.3d 493, 502 (Tex. App. 2002) ("Non-disclosure without evidence that a defendant had knowledge of the undisclosed information and intentionally withheld the information is not actionable." (citation omitted)). As discussed above, Plaintiffs have alleged that, despite knowing of the vulnerabilities in their data collection practices and despite take efforts to remediate those shortcomings, Defendants, who shared representations regarding data security with Plaintiffs, did not disclose the serious risk of exposure of Plaintiffs' PII. Am. Compl. ¶¶ 46-84, 90-97.

Therefore, based on the above, the Court finds that Texas Plaintiff Palencia have sufficiently alleged a claim under the DTPA.

v. Washington

Washington Plaintiff Sara Sharp, individually and on behalf of the Washington subclass, alleges a claim under the Washington Consumer Protection Act ("WCPA"), RCW §§ 19.86.020, *et seq*.

Section 19.86.020 prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." RCW § 19.86.020. The purpose of the statute is to "complement the body of federal law governing restraints of trade, unfair competition and unfair, deceptive, and fraudulent acts and practices in order to protect the public

and foster fair and honest competition." *Id.*; *Haberman v. Wash. Pub. Power Supply Sys.*, 744 P.2d 1032 (Wa. 1987). And in that regard, the WCPA is to be "liberally construed [such] that its beneficial purposes may be served." RCW 19.86.920; *see also Short v. Demopolis*, 103 Wn.2d 52, 61, 691 P.2d 163 (Wa. 1984). Moreover, that statute states that "[a]ny person who is injured in his or her business or property" by a violation of the act may bring a civil suit for injunctive relief, damages, attorney fees and costs, and treble damages. RCW 19.86.090. Thus, a private individual can bring suit under the WCPA. To prevail in a private WCPA claim, the plaintiff must prove (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) affecting the public interest, (4) injury to a person's business or property, and (5) causation. *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 105 Wn.2d 778, 784, 719 P.2d 531 (Wa. 1986).

In moving to dismiss this claim, Defendants argue that Plaintiff Sharp has failed to allege an actual injury or damages, liability cannot be premised on an alleged omission, and have failed, as required, to allege fraud with particularity. *See* [Doc. 387] at 43-45; *id*. at n.22. But none of these arguments is persuasive.

First, for the reasons already discussed, Plaintiffs have alleged a satisfactory injury. As with the other statutes, Washington requires a private WCPA plaintiff to establish the alleged deceptive act caused injury. *See Hangman*, 105 Wn. at 794. And while personal injuries, as opposed to injuries to "business or property," do not satisfy the statute's injury requirement, *see Stevens v. Hyde Athletic Indus., Inc.*, 54 Wn. App. 366, 370, 773 P.2d 871 (Wa. 1989), the injury requirement is met upon proof that the plaintiff's "property interest or money is diminished because of the unlawful conduct even if the expenses caused by the statutory violation are minimal." *Mason v. Mortgage Am., Inc.*, 114 Wn.2d 842, 854, 792 P.2d 142 (Wa. 1990)

(temporary loss of use of property while brokerage company improperly withheld title constituted sufficient injury to support attorney fee award under the WCPA). Thus, by way of example, undertaking tasks or incurring expenses to respond to the alleged deceptive practice, including costs incurred in response to data breach, which may affect individual time or business profits, qualifies as a cognizable injury. *See Panag v. Farmers Ins. Co. of Wash.*, 166 Wn.2d 27, 65, 204 P.3d 885, 903 (Wa. 2009) (collecting cases); *see also Mason v. Mortg. Am., Inc.*, 114 Wn.2d 842, 854, 792 P.2d 142 (Wa. 1990) (the injury requirement is met upon proof the plaintiff's "property interest or money is diminished because of the unlawful conduct even if the expenses caused by the statutory violation are minimal").

Here, Plaintiff Sharp applied for and used a Capital One credit card, providing her PII to Capital One in order to do so. Am. Compl. ¶ 27. After the Data Breach, she suffered identity theft and fraud in the form of unauthorized charges on her bank account and fraudulent charges under her name. *Id*. As a result, Plaintiff Sharp spent time investigating the source of the fraud and unauthorized charges and she continues to spend time and effort regularly monitoring her accounts to detect fraudulent activity. *Id*. Based on the above, the Court concludes that Sharp has adequately alleged an injury under the WCPA. *See Panag*, 204 P.3d at 902 (investigation expenses and other costs resulting from a deceptive business practice sufficiently establish injury) (citing *State Farm Fire & Cas. Co. v. Quang Huynh*, 92 Wn. App. 454, 470, 962 P.2d 854 (Wa. 1998) (although insurance company did not pay chiropractor's false billing statements, it sufficiently established injury by proving it "incurred expenses for experts, interpreters, transcribers, attorneys, and its own employees during its investigation").

Defendants separately argue that Sharp cannot allege a claim under the WCPA because Plaintiffs' alleged omission cannot qualify as a proscribed deceptive act. *See* [Doc. 387] at 44 n.

22. This issue reduces to what can qualify, for purposes of the WCPA, as an "unfair" or "deceptive" act. Whether an act is "unfair" or "deceptive" is a question of law. *See Leingang v. Pierce County Med. Bureau, Inc.*, 131 Wn.2d 133, 150, 930 P.2d 288 (Wa. 1997).

In deciding whether a practice was "unfair" or "deceptive," Washington state courts may consider federal court decisions that have approved or rejected administrative determinations made by the FTC in enforcing the FTC Act. *See* RCW 19.86.920 ("It is the intent of the legislature that, in construing this act, the courts be guided by final decisions of the federal courts and final orders of the federal trade commission interpreting the various federal statutes dealing with the same or similar matters."). In that regard, federal courts, reviewing the FTC's enforcement actions, have rejected the argument, advanced by Defendants here, that a communication cannot be deceptive if it includes an omission. *See, e.g., Sw. Sunsites, Inc. v. Fed. Trade Comm'n*, 785 F.2d 1431, 1435 (9th Cir. 1986) ("Indeed, a communication may contain accurate information yet be deceptive.") (emphasis omitted). Following this precedent, Washington courts have concluded that a misrepresentation of the material terms of a transaction or the *failure to disclose* material terms violates the WCPA. *See, e.g., State v. Ralph Williams' Nw. Chrysler Plymouth, Inc.*, 87 Wn.2d 298, 305-09, 553 P.2d 423 (Wa. 1976). Based on this precedent, the Court finds that an omission can ground a consumer claim under the WCPA.[36]

Therefore, for the foregoing reasons, the Court concludes that the Washington Plaintiff has plausibly stated a claim under the WCPA.

[36] Assuming that a claim under the WCPA must be pled with particularity, for the same reasons discussed with respect to Plaintiffs' UCL claim, the allegations in the Complaint are pled with sufficient particularity to satisfy Rule 9(b).

IV. CONCLUSION

Accordingly, for the foregoing reasons, it is hereby

ORDERED that Defendant Capital One's Motion [Doc. 386] and Defendant Amazon's Motion to Dismiss [Doc. 394] be, and the same hereby are, **GRANTED** in part and **DENIED** in part, as follows:

1. As to Count 1 (negligence), the negligence claims under the laws of Washington are dismissed; and the Motions are otherwise denied;
2. As to Count 2 (negligence *per se*), the negligence *per se* claims under the laws of California, Florida, Texas, Virginia, and Washington are dismissed; and the Motions are otherwise denied;
3. As to Count 3 (unjust enrichment), the Motions are denied;
4. As to Count 4 (declaratory judgment), the Motions are denied;
5. As to Count 5 (breach of confidence), the breach of confidence claims under the laws of California, New York, Texas, Virginia, and Washington are dismissed; and the Motions are otherwise denied;
6. As to Count 6 (breach of contract), the Capital One Motion is denied;
7. As to Count 7 (breach of implied contract), the Capital One Motion is denied;
8. As to Count 8 (California Unfair Competition Law), the Motions are denied;
9. As to Count 9 (California Consumer Legal Remedies Act), the Motions are denied;
10. As to Count 10 (Florida Deceptive and Unfair Trade Practices Act), the claim against Capital One is dismissed as abandoned; and the Motions are otherwise denied;
11. As to Count 11 (New York General Business Law (Count 11), the Motions are denied;

12. As to Count 12 (Texas Deceptive Trade Practices Act—Consumer Protection Act (Count 12), the Motions are denied;

13. As to Count 13 (Virginia Personal Information Breach Notification Act), the Motions are denied;

14. As to Count 14 (Washington Data Breach Notification Act), the Motions are denied; and

15. As to Count 15 (Washington Consumer Protection Act), the Motions are denied.

The Clerk is directed to forward copies of this Order to all counsel of record.

/s/
Anthony J. Trenga
United States District Judge

Alexandria, Virginia
September 18, 2020