IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2800 1:17-md-2800-TWT CONSUMER CASES

OPINION AND ORDER

This is a data breach case. It is before the Court on the Defendants' Motion to Dismiss the Consolidated Consumer Class Action Complaint [Doc. 425]. For the reasons set forth below, the Defendants' Motion to Dismiss the Consolidated Consumer Class Action Complaint [Doc. 425] is GRANTED in part and DENIED in part.

I. Background

On September 7, 2017, the Defendant Equifax Inc. announced that it was the subject of one of the largest data breaches in history.[1] From mid-May through the end of July 2017, hackers stole the personal and financial information of nearly 150 million Americans.[2] During this time period, Equifax failed to detect the hackers' presence in its systems, allowing the hackers to exfiltrate massive amounts of sensitive personal data that was in the company's

[1] Consolidated Consumer Class Action Compl. ¶ 2 [Doc. 374].

[2] *Id.*

custody.[3] This data breach ("Data Breach") is unprecedented – it affected almost half of the entire American population.[4] The Data Breach was also severe in terms of the type of information that the hackers were able to obtain. The hackers stole at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers.[5] This is extremely sensitive personal information. Using this information, identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness.[6]

Equifax Inc. is a Georgia corporation with its principal place of business in Atlanta, Georgia.[7] Equifax is the parent company of the Defendants Equifax Information Services LLC and Equifax Consumer Services LLC.[8] Both of those subsidiary companies are Georgia limited liability companies, with their principal places of business in Atlanta, Georgia.[9] The Defendants operate

---

3 *Id.* ¶ 2.

4 *Id.* ¶ 4.

5 *Id.*

6 *Id.*

7 *Id.* ¶ 109.

8 *Id.*

9 *Id.* ¶¶ 110-11.

together as an integrated consumer reporting agency.[10] The Plaintiffs are 96 consumers who allege that they have been injured by the Data Breach. They allege that they are suffering a "present, immediate, imminent, and continuing increased risk of harm" due to the compromise of their personally identifiable information in the Data Breach.[11] The Plaintiffs seek to represent a class of those similarly situated consumers in the United States who were injured by the Data Breach.[12]

Equifax's business model entails aggregating data relating to consumers from various sources, compiling that data into credit reports, and selling those reports to lenders, financial companies, employers, and others.[13] Credit reporting agencies are "linchpins" of the nation's financial system due to the importance of credit reports in decisions to extend credit.[14] Equifax also sells this information directly to consumers, allowing consumers to purchase their credit files and credit scores.[15] In recent years, Equifax has worked to rapidly grow its business. Recognizing the value in obtaining massive troves of consumer data, Equifax has aggressively acquired companies with the goal of

---

10 *Id.* ¶ 112.

11 *Id.* ¶ 11.

12 *Id.*

13 *Id.* ¶ 134.

14 *Id.*

15 *Id.* ¶ 135.

expanding into new markets and acquiring new sources of data.[16] Equifax now maintains information on over 820 million individuals and 91 million businesses worldwide.[17]

Equifax recognized the importance of data security, and the value of the data in its custody to cybercriminals. Equifax observed other major, well-publicized data breaches, including those at Target, Home Depot, Anthem, and its competitor Experian.[18] Equifax held itself out as a leader in confronting such threats, offering "data breach solutions" to businesses.[19] It also acquired two identity theft protection companies, Trusted ID and ID Watchdog.[20] Equifax was also the subject of several prior data breaches. From 2010 on, Equifax suffered several different data breach incidents highlighting deficiencies in its cybersecurity protocol.[21] Given these prior breaches, cybersecurity experts concluded that Equifax was susceptible to a major data breach.[22] Analyses of Equifax's cybersecurity demonstrated that it lacked basic maintenance

---

16 *Id.* ¶ 137.

17 *Id.* ¶ 144.

18 *Id.* ¶¶ 146, 159-65.

19 *Id.* ¶ 147.

20 *Id.* ¶ 146.

21 *Id.* ¶¶ 166-82.

22 *Id.* ¶¶ 177-82.

techniques that are highly relevant to potential data breaches.[23] However, despite these risks, Equifax did little to improve its cybersecurity practices. Equifax's leaders afforded low priority to cybersecurity, spending a small fraction of the company's budget on cybersecurity.[24]

The story of the Data Breach begins on March 6, 2017. On that date, a serious vulnerability in the Apache Struts software was discovered and reported.[25] This software, a popular open-source program, was used by Equifax in its consumer dispute portal website.[26] The next day, the Apache Software Foundation issued a free patch and urged all users to immediately implement the patch.[27] The Department of Homeland Security also issued warnings concerning this vulnerability.[28] Equifax internally disseminated the warning, but never implemented the patch.[29] Then, beginning on May 13, 2017, hackers were able to manipulate the Apache Struts vulnerability to access Equifax's systems, and using simple commands determined the credentials of network accounts that allowed them to access the confidential information of millions of

---

23 *Id.* ¶ 178.

24 *Id.* ¶ 216.

25 *Id.* ¶¶ 183-86.

26 *Id.* ¶ 184.

27 *Id.* ¶ 187.

28 *Id.* ¶ 188.

29 *Id.* ¶ 189.

American consumers.[30] From May 13 to July 30, 2017, the hackers remained undetected in Equifax's systems.[31] During this time, the hackers were able to steal the sensitive personally identifiable information of approximately 147.9 million American consumers.[32] The personally identifiable information that hackers obtained in the Data Breach includes names, addresses, birth dates, Social Security numbers, driver's license information, telephone numbers, email addresses, tax identification numbers, credit card numbers, credit report dispute documents, and more.[33]

On July 29, 2017, Equifax's security team noticed "suspicious network traffic" in the dispute portal.[34] The next day, the consumer dispute portal was deactivated and taken offline.[35] On July 31, 2017, Equifax's CEO Richard Smith was informed of the breach.[36] On August 2, 2017, Equifax informed the Federal Bureau of Investigation about the Data Breach, and retained legal counsel to guide its investigation.[37] Equifax also hired cybersecurity firm Mandiant to

---

30 *Id.* ¶ 195.

31 *Id.*

32 *Id.* ¶ 195.

33 *Id.* ¶ 11.

34 *Id.* ¶¶ 196-97.

35 *Id.* ¶ 197.

36 *Id.* ¶ 198.

37 *Id.* ¶ 201.

investigate the suspicious activity.[38] On September 7, 2017, seven weeks after discovering suspicious activity, Equifax publicly disclosed the Data Breach in a press release.[39] Experts have since opined that the Data Breach was the result of weak cybersecurity measures and Equifax's low priority for data security.[40]

The Plaintiffs here are a putative class of consumers whose personal information was stolen during the Data Breach. The class alleges that it has been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. The putative class brings a number of nationwide claims, along with a number of state claims. The class also seeks declaratory and injunctive relief. The Defendants now move to dismiss.

II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief.[41] A complaint may survive a motion to dismiss for failure to state a claim, however,

---

38 *Id.*

39 *Id.* ¶ 227.

40 *Id.* ¶¶ 214-226.

41 *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009); FED. R. CIV. P. 12(b)(6).

even if it is "improbable" that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely "remote and unlikely."[42] In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff.[43] Generally, notice pleading is all that is required for a valid complaint.[44] Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests.

III. Discussion

A. Choice of Law

First, the Court concludes that Georgia law governs this case. This case is before the Court based on diversity jurisdiction. The Court therefore looks to Georgia's choice of law rules to determine the appropriate rules of decision.[45] Georgia follows the traditional approach of *lex loci delecti* in tort cases, which generally applies the substantive law of the state where the last event occurred

---

[42] *Bell Atlantic v. Twombly*, 550 U.S. 544, 556 (2007).

[43] *See Quality Foods de Centro America, S.A. v. Latin American Agribusiness Dev. Corp., S.A.*, 711 F.2d 989, 994-95 (11th Cir. 1983); *see also Sanjuan v. American Bd. of Psychiatry and Neurology, Inc.*, 40 F.3d 247, 251 (7th Cir. 1994) (noting that at the pleading stage, the plaintiff "receives the benefit of imagination").

[44] *See Lombard's, Inc. v. Prince Mfg., Inc.*, 753 F.2d 974, 975 (11th Cir. 1985), *cert. denied*, 474 U.S. 1082 (1986).

[45] *Frank Briscoe Co., Inc. v. Ga. Sprinkler Co., Inc.*, 713 F.2d 1500, 1503 (11th Cir.1983) ("A federal court faced with the choice of law issue must look for its resolution to the choice of law rules of the forum state.").

necessary to make an actor liable for the alleged tort.[46] Usually, this means that the "law of the place of the injury governs rather than the law of the place of the tortious acts allegedly causing the injury."[47] However, there is an exception when the law of the foreign state is the common law. "[T]he application of another jurisdiction's laws is limited to statutes and decisions construing those statutes. When no statute is involved, Georgia courts apply the common law as developed in Georgia rather than foreign case law."[48] The Plaintiffs identify no foreign statutes that govern their common law claims. Therefore, the Court will apply Georgia law to the common law claims.[49]

B. Fair Credit Reporting Act

The Defendants first move to dismiss the Consumer Plaintiffs' claims

---

[46] *Dowis v. Mud Slingers, Inc.*, 279 Ga. 808, 816 (2005); *Int'l Bus. Machines Corp. v. Kemp*, 244 Ga. App. 638, 640 (2000).

[47] *Mullins v. M.G.D. Graphics Sys. Grp.*, 867 F. Supp. 1578, 1581 (N.D. Ga. 1994).

[48] *In re Tri-State Crematory Litig.*, 215 F.R.D. 660, 677 (N.D. Ga. 2003) (internal quotations omitted). The Georgia Supreme Court has recently reaffirmed this exception. *See Coon v. The Med. Ctr., Inc.*, 300 Ga. 722, 729 (2017) ("In the absence of a statute, however, at least with respect to a state where the common law is in force, a Georgia court will apply the common law as expounded by the courts of Georgia.").

[49] The Plaintiffs argue that Georgia law should apply unless the Court decides "that Georgia law is adverse to the common law claims of the national class pled in the Complaint, in which case it will be necessary to consider the common law of each state applicable to the proposed alternative, state-specific classes." Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 9. However, the Plaintiffs cite no authority for such a proposition. The Court concludes that Georgia law will govern this case.

under the Fair Credit Reporting Act ("FCRA"). Under the FCRA, a "consumer reporting agency may furnish a consumer report" only under limited circumstances provided for in the statute.[50] In Count 1 of the Complaint, the Consumer Plaintiffs allege that the Defendants "furnished Class members' consumer reports" in violation of section 1681b of the FCRA and "failed to maintain reasonable procedures designed to limit the furnishing of Class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of Class members' consumer reports to unauthorized entities or computer hackers" in violation of section 1681e of the FRCA.[51] The Defendants move to dismiss, arguing that Equifax did not "furnish" any consumer information within the meaning of the statute, and that the stolen personally identifying information is not a "consumer report" within the meaning of the statute.[52] They also argue that since the Consumer Plaintiffs' section 1681b claim fails to state a claim, their section 1681e also necessarily fails.[53] The Court agrees that the Consumer Plaintiffs fail to state a claim under the FCRA.

First, the Defendants argue that Equifax did not "furnish" the Plaintiffs' personal information within the meaning of the FCRA. The FCRA provides that

---

[50] 15 U.S.C. § 1681b(a).

[51] Consolidated Consumer Class Action Compl. ¶¶ 321, 324.

[52] Defs.' Mot. to Dismiss, at 12-15.

[53] *Id.* at 15-16.

a consumer reporting agency may only "furnish" a consumer report under limited circumstances.[54] However, the statute does not further define "furnish." Generally, courts have held that information that is stolen from a credit reporting agency is not "furnished" within the meaning of the FCRA. For example, in *In re Experian Data Breach Litigation*, the court explained that "[a]lthough 'furnish' is not defined in the FCRA, courts generally use the term to describe the active transmission of information to a third-party rather than a failure to safeguard the data."[55] In such a case, the data is stolen by a third party, and not furnished to the third party.[56] Other courts have come to the same conclusion.[57] The Plaintiffs acknowledge that the caselaw supports Equifax's argument, but contend nonetheless that Equifax's conduct was "so egregious" that it should be considered akin to furnishing.[58] The Plaintiffs fail to offer a discernable criteria by which to determine when conduct becomes so egregious that it becomes akin to furnishing. Even assuming Equifax's conduct was egregious, the Court concludes that the Plaintiffs have not alleged facts

---

[54] 15 U.S.C. § 1681b(a).

[55] *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595, at *2 (C.D. Cal. Dec. 29, 2016) (quoting *Dolmdage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *3 (N.D. Ill. Jan. 21, 2015)).

[56] *Id.*

[57] *See, e.g.*, *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118, 2017 WL 4987663, at *4 (S.D. Ohio Aug. 16, 2017).

[58] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 46-47.

showing that Equifax "furnished" the Plaintiffs' consumer reports to the hackers.

Next, the Defendants argue that the personally identifying information stolen during the Data Breach is not a "consumer report" within the meaning of the FCRA.[59] The Court agrees. Section 1681b of the FCRA prohibits the furnishing of "consumer reports," except under limited circumstances.[60] The FCRA defines "consumer report," in general, to mean:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for--(A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.[61]

Equifax argues – and the Plaintiffs do not dispute this – that the hackers did not obtain access to the active credit files maintained by one of the Equifax subsidiaries. The hackers got only "legacy" data. Courts, facing similar factual circumstances, have concluded that information such as that taken in the Data Breach does not constitute a "consumer report," but instead is "header

---

[59] Defs.' Mot. to Dismiss, at 13-15.

[60] 15 U.S.C. § 1681b.

[61] 15 U.S.C. § 1681a(d)(1).

information."[62] Such information is not a "consumer report" because it does not bear on an individual's credit worthiness.[63] Information, such as a consumer's "name, phone number, social security number, date of birth, driver's license, current address, and time spent at that address" does not, itself, constitute such a credit report.[64] The Plaintiffs' argument that the information stolen in the Data Breach could bear on their credit worthiness is not persuasive. Therefore, the Court concludes that the Plaintiffs fail to allege facts showing that the information stolen was a "credit report."

Finally, since the Consumer Plaintiffs' section 1681b claim fails, their section 1681e claim must also necessarily fail. Section 1681e requires consumer reporting agencies to "maintain reasonable procedures designed to avoid violations of section 1681c of this title and to limit the furnishing of consumer reports to the purposes listed under section 1681b of this title."[65] However, a plaintiff bringing a claim that a reporting agency violated the "reasonable procedures" requirement of section 1681e must first show that the reporting

---

[62] *See, e.g.*, *Parker v. Equifax Info. Servs., LLC*, No. 2:15-cv-14365, 2017 WL 4003437, at *3 (E.D. Mich. Sept. 12, 2017).

[63] *Id.* ("The accumulation of biographical information from Equifax's products does not constitute a consumer report because the information does not bear on Parker's credit worthiness.").

[64] *Id.* at *1, *3.

[65] 15 U.S.C. § 1681e.

agency released the report in violation of section 1681b.[66] Therefore, since the Plaintiffs' claims under section 1681b fail, their claims under section 1681e also fail.

Next, two Plaintiffs, Grace Cho and Debra Lee, bring claims under 15 U.S.C. § 1681g(a).[67] These Plaintiffs, referred to as the "FCRA Disclosure Subclass" in the Complaint, allege that the Defendants violated sections 1681(a)(1) and 1681(a)(3) of the FCRA by failing to clearly and accurately disclose all of the information in their consumer files after requesting Equifax to do so.[68] According to these Plaintiffs, the Defendants violated this statute by failing to identify the Data Breach and the individuals who procured their information, namely the hackers.[69] However, as explained above, the hackers did not obtain a "consumer report" within the meaning of the FCRA. And Equifax could not be expected to disclose the identity of the unknown hackers. Therefore, this claim should be dismissed.

C. Legally Cognizable Injury

The Defendants next argue that all of the Plaintiffs' tort claims, including their negligence, negligence per se, and state consumer protection act violations,

---

66 *Experian*, 2016 WL 7973595, at *2 (quoting *Moreland v. CoreLogic SafeRent LLC*, No. SACV 13-470 AG, 2013 WL 5811357, at *6 (C.D. Cal. Oct. 25, 2013)).

67 Consolidated Consumer Class Action Compl. ¶¶ 417-27.

68 *Id.* ¶¶ 418-20.

69 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 50-51.

fail because they have not sufficiently alleged injury and proximate causation.[70] According to the Defendants, the Plaintiffs' injuries are not legally cognizable harms, and even if they were, the Plaintiffs have failed to adequately allege that the Defendants proximately caused their harms.[71] Finally, the Defendants argue that the Plaintiffs' tort claims are all barred by the economic loss doctrine.

1. Non-Harms and Speculative Future Harms

First, the Defendants contend that the Plaintiffs have not pleaded legally cognizable harms because their purported injuries only include "non-harms" and "speculative future harms."[72] "It is well-established Georgia law that before an action for a tort will lie, the plaintiff must show he sustained injury or damage as a result of the negligent act or omission to act in some duty owed to him."[73] "Although nominal damages can be awarded where there has been an injury but the injury is small, . . . where there is no evidence of injury accompanying the tort, an essential element of the tort is lacking, thereby entitling the defendant

---

[70] Defs.' Mot. to Dismiss, at 16. Importantly, the Defendants do not seem to contend that the Plaintiffs have failed to establish standing. Instead, the Defendants contend that the Plaintiffs have not established a legally cognizable harm, or proximate causation, as elements of a tort claim. The Plaintiffs highlight this distinction in their brief. *See* Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 19 ("Equifax does not dispute standing and instead argues that Plaintiffs fail to plead 'legally cognizable harms' under Georgia law."). The Defendants do not disagree.

[71] *Id.*

[72] *Id.*

[73] *Whitehead v. Cuffie*, 185 Ga. App. 351, 353 (1987).

to judgment in his favor."[74]

The Defendants first contend that the compromise of personally identifiable information itself is not an injury.[75] Each of the Plaintiffs alleges that his or her personally identifiable information was compromised in the Data Breach.[76] Such an injury is legally cognizable under Georgia law.[77] The cases relied upon by the Defendants are distinguishable. The Defendants cite *Rite Aid of Georgia, Inc. v. Peacock* for the proposition that a plaintiff suffers no injury from the illegal sale of personally identifiable information.[78] However, as the Plaintiffs point out, the plaintiff in that case did not allege that this information was misused, or likely to be misused.[79] In *Rite Aid*, the plaintiff's pharmacy records were sold from Rite Aid to Walgreens when a Rite Aid store was closing.[80] The plaintiff sought certification of a class of all individuals whose information had been sold to Walgreens.[81] The court concluded that class

---

74 *Id.*

75 Defs. Mot. to Dismiss, at 17.

76 *See* Consolidated Consumer Class Action Compl. ¶¶ 13-108.

77 *See, e.g., In re Arby's Restaurant Grp. Inc. Litig.,* No. 1:17-cv-0514-AT, 2018 WL 2128441, at *11 (N.D. Ga. Mar. 5, 2018).

78 Defs.' Mot. to Dismiss, at 17.

79 *See Rite Aid of Ga, Inc. v. Peacock*, 315 Ga. App. 573, 580 (2012).

80 *Id.* at 573.

81 *Id.* at 574.

certification was not proper, in part, because the plaintiff had not alleged an injury from the sale of his information from one pharmacy to the other, and instead only alleged a violation of law.[82] In contrast, the Plaintiffs here have alleged that they have been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. These allegations of actual injury are sufficient to support a claim for relief.[83]

The Defendants also cite *Finnerty v. State Bank & Trust Company* for the proposition that fear of future damages from identity theft is too speculative to form a basis of recovery.[84] However, as the Plaintiffs emphasize, that case involved an invasion of privacy claim by an individual whose Social Security number was included in a public court filing.[85] The court concluded that this claim failed because, to state a claim for invasion of privacy, a plaintiff must

---

[82] *Id.* at 576.

[83] *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016); *In re Arby's Rest. Grp. Inc. Litig.*, 317 F. Supp. 3d 1222 (N.D. Ga. 2018).

[84] Defs.' Mot. to Dismiss, at 17.

[85] *Finnerty v. State Bank & Trust Co.*, 301 Ga. App. 569 (2009), *disapproved of in part on other grounds by Cumberland Contractors, Inc. v. State Bank & Trust Co.*, 327 Ga. App. 121, 126 n.4 (2014).

show that there was a public disclosure in which information is distributed to the public at large.[86] There, the claimant failed to allege that anyone actually saw his Social Security number, and thus did not prove that there was a public disclosure.[87] Thus, the court there did not hold that the disclosure of personal information is, as a matter of law, not a legally cognizable injury. Instead, it concluded that one of the elements of an invasion of privacy claim was not met, making it distinguishable from this case.[88] And, in contrast to the inadvertent disclosure of a Social Security number in a single public court filing, the compromise of a huge amount of personally identifying information by criminal hackers presents a much more significant risk of identity fraud.

The Defendants also cite *Randolph v. ING Life Insurance and Annuity Company.*[89] There, the plaintiffs sued after a laptop computer containing their personal information was stolen from the home of one of the defendant's employees, alleging that there was a substantial risk of identity theft and other dangers due to the possible unauthorized use of their personal information.[90] In that case, there was no evidence that the theft occurred for the specific purpose

---

86 *Id.* at 571.

87 *Id.* at 571-72.

88 *Id.*

89 Defs.' Mot. to Dismiss, at 18.

90 *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 704 (D.C. 2009).

of obtaining the information on the laptop as opposed to the computer itself. Here, by contrast, the Plaintiffs allege that their information was specifically targeted and has already been misused. The Plaintiffs have adequately alleged facts showing actual cognizable injury.

The Defendants also cite *Collins v. Athens Orthopedic Clinic* in their reply brief.[91] There, the defendant's patients sued after a cyberhacker stole their personal information from the defendant's systems.[92] The court concluded that the plaintiffs did not allege a legally cognizable harm.[93] It explained that:

> Plaintiffs allege that their information has been compromised and that they have spent time placing fraud or credit alerts on their accounts and "anticipate" spending more time on these activities. Plaintiffs claim damages, specifying only the cost of identity theft protection, credit monitoring, and credit freezes to be maintained "over the course of a lifetime." While credit monitoring and other precautionary measures are undoubtedly prudent, we find that they are not recoverable damages on the facts before us because Plaintiffs seek only to recover for an increased risk of harm.[94]

Thus, according to the Defendants, the Plaintiffs' claims must fail, since costs associated with protecting the plaintiffs' personal information in *Collins* failed to establish a sufficient injury.[95]

However, *Collins* is distinguishable. There, the plaintiffs alleged only an

---

91 Defs.' Reply Br., at 9.

92 *Collins v. Athens Orthopedic Clinic*, 347 Ga. App. 13 (2018).

93 *Id.* at 18.

94 *Id.*

95 Defs.' Reply Br., at 9.

"increased risk of harm" associated with taking precautionary measures.[96] The mere risk of harm, and not the type of injuries alleged, led the court to conclude that the plaintiffs' allegations as to injuries failed. In contrast, the Plaintiffs here have not pleaded merely an increased risk of harm. Instead, they have alleged that they have already incurred significant costs in response to the Data Breach. Many of the Plaintiffs have also already suffered forms of identity theft. Moreover, the Plaintiffs here have sufficiently alleged a substantial and imminent risk of impending identity fraud due to the vast amount of information that was obtained in the Data Breach. The Court concludes that these allegations are sufficient.

The Defendants also argue that the Plaintiffs that allege payment card fraud have failed to allege a sufficient injury.[97] Plaintiffs Alvin Alfred Kleveno Jr., Maria Martucci, and Robert J. Etten allege that they experienced unauthorized charges on their payment cards as a result of the Data Breach.[98] The Defendants contend that these allegations are insufficient because these Plaintiffs have not alleged the date on which these fraudulent charges were made, and because they failed to allege that they were not reimbursed for those charges.[99] However, under Rule 8's requirement of a plain and simple statement,

---

96 *Collins*, 347 Ga. App. at 18.

97 Defs.' Mot. to Dismiss, at 19-20.

98 Consolidated Consumer Class Action Compl. ¶¶ 26, 33, 60.

99 Defs.' Mot. to Dismiss, at 19.

these Plaintiffs need not allege the specific date on which these fraudulent charges occurred. The Plaintiffs' allegations that such charges occurred are sufficient, and the Defendants cite no authority holding otherwise. Furthermore, contrary to the Defendants' assertions, these Plaintiffs also need not allege that they were not reimbursed for these fraudulent charges to adequately allege an injury.[97] The Plaintiffs' allegations that they suffered unauthorized charges on their payment cards as a result of the Data Breach are actual, concrete injuries that are legally cognizable under Georgia law.

2. Proximate Causation

The Defendants next contend that the Plaintiffs have failed to adequately allege that Equifax proximately caused their injuries.[98] "[B]efore any negligence, even if proven, can be actionable, that negligence must be the proximate cause of the injuries sued upon."[99] "To establish proximate cause, a plaintiff must show a legally attributable causal connection between the defendant's conduct and the alleged injury."[100] A plaintiff must establish "that it is more likely than not that

---

97 *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012) (explaining that, under notice pleading standards, plaintiffs need not allege that they experienced "unreimbursed losses" as a result of payment card fraud).

98 Defs.' Mot. to Dismiss, at 20-21.

99 *Anderson v. Barrow Cty.*, 256 Ga. App. 160, 163 (2002).

100 *Id.*

the conduct of the defendant was a cause in fact of the result."[101] "A mere possibility of such causation is not enough; and when the matter remains one of pure speculation or conjecture, or the probabilities are at best evenly balanced, it becomes the duty of the court to grant summary judgment for the defendant."[102]

First, the Defendants argue that the Plaintiffs fail to allege that any injuries resulting from identity theft, payment-card fraud, or other similar theories resulted specifically from the Equifax Data Breach, and not some other data breach or fraudulent conduct.[103] According to the Defendants, the Plaintiffs highlight dozens of other security breaches dating to 2013 in the Complaint, and the Defendants assert that over 1,500 data breaches occurred in 2017 alone. Thus, since the Plaintiffs have failed to allege that their injuries resulted directly from their personal information being obtained in this specific Data Breach, their theory of causation is "guesswork at best."[104]

However, the Court finds this argument unpersuasive. Many of the Plaintiffs have alleged in the Complaint that they suffered some form of identity

---

101 *Grinold v. Farist*, 284 Ga. App. 120, 121 (2007) (quoting *Feazell v. Gregg*, 270 Ga. App. 651, 655 (2004)).

102 *Id.* at 121-22.

103 Defs.' Mot. to Dismiss, at 21.

104 *Id.*

theft or other fraudulent activity as a result of the Data Breach.[105] Such an allegation is sufficient at the pleading stage to establish that the Data Breach was the proximate cause of this harm. The Plaintiffs need not explicitly state that other breaches did *not* cause these alleged injuries, since their allegations that this Data Breach *did* cause their injuries implies such an allegation. Furthermore, allowing the Defendants "to rely on other data breaches to defeat a causal connection would 'create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable.'"[106] The Court declines to create such a perverse incentive.

Many of the Plaintiffs also allege in the Complaint that they purchased credit monitoring and incurred other costs in direct response to the Data Breach.[107] Thus, even assuming their identity theft injuries resulted from previous breaches, these separate injuries resulted only from the occurrence of the Data Breach. Finally, even assuming that such an argument could disprove

---

[105] *See, e.g.*, Consolidated Consumer Class Action Compl. ¶ 17 ("As a result of the breach, Plaintiff Sanchez has suffered identity theft in the form of an unauthorized credit card opened in his name using his Personal Information.").

[106] *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *19 (N.D. Cal. Aug. 30, 2017) (quoting *In re Anthem, Inc. Data Breach Litig.*, 162. F. Supp. 3d 953, 988 (N.D. Cal. 2016)).

[107] *See, e.g.*, Consolidated Consumer Class Action Compl. ¶ 15 ("[A]s a result of the breach, Plaintiff Bishop paid to maintain his credit monitoring services from TransUnion and Experian in order to mitigate possible harm and spent time and effort monitoring his accounts for fraudulent activity.").

proximate causation, it presents a factual dispute most appropriate for a jury to consider. The Plaintiffs have alleged that the Data Breach caused their identities to be stolen, while the Defendants contend prior breaches caused these injuries. This is purely a dispute of fact that is not appropriate for resolution at this stage of the litigation.[108] Therefore, the Court concludes that the Plaintiffs have adequately alleged that the Data Breach proximately caused their injuries. The Plaintiffs plausibly allege that Equifax had custody of their personally identifiable information, that Equifax's systems were hacked, that these hackers obtained this personal information, and that as a result of this breach, they have become the victims of identity theft and other fraudulent activity. This is sufficient.

Next, the Defendants contend that the Plaintiffs' injuries were proximately caused by an "unidentified third party's criminal acts," and not Equifax itself.[109] According to the Defendants, the unforeseeable criminal acts of third parties "insulate" defendants from liability.[110] "Generally, there is no duty to prevent the unforeseeable 'intervening criminal act of a third person.'"[111]

---

[108] The Court also declines to consider the Defendants' argument that over 1,500 data breaches occurred in 2017. Even if this is true, this assertion has no basis in the allegations of the Complaint, and should not be considered at this stage of the litigation.

[109] Defs.' Mot. to Dismiss, at 21-22.

[110] *Id.* at 22.

[111] *In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *3 (N.D. Ga. Mar. 5, 2018) (quoting *Bradley Center, Inc. v.*

Under Georgia law, "when a defendant claims that its negligence is not the proximate cause of the plaintiff's injuries, but that an act of a third party intervened to cause those injuries, the rule is 'that an intervening and independent wrongful act of a third person producing the injury, and without which it would not have occurred, should be treated as the proximate cause, insulating and excluding the negligence of the defendant.'"[112]

However, "this rule does not insulate the defendant 'if the defendant had reasonable grounds for apprehending that such wrongful act would be committed.'"[113] "[I]f the character of the intervening act claimed to break the connection between the original wrongful act and the subsequent injury was such that its probable or natural consequences could reasonably have been anticipated, apprehended, or foreseen by the original wrong-doer, the causal connection is not broken, and the original wrong-doer is responsible for all of the consequences resulting from the intervening act."[114] Thus, if the Defendants had reasonable grounds to anticipate the criminal act, then they are not insulated from liability. "In determining whether a third party criminal act is foreseeable, Georgia courts have held that 'the incident causing the injury must be

---

Wessner, 250 Ga. 199, 201 (1982)).

[112] *Goldstein, Garber, & Salama, LLC v. J.B.*, 300 Ga. 840, 841 (2017) (quoting *Ontario Sewing Mach. Co., Ltd. v. Smith*, 275 Ga. 683, 686 (2002)).

[113] *Id.* (quoting *Ontario Sewing Mach.*, 275 Ga. at 686).

[114] *Id.* at 842 (internal quotations omitted).

substantially similar in type to the previous criminal activities . . . so that a reasonable person would take ordinary precautions to protect his or her customers or tenants against the risk posed by that type of activity.'"[115] The question of reasonable foreseeability of a criminal attack is generally for a jury to determine.[116] However, it may not be in this case because of the many public statements by Equifax that it knew how valuable its information was to cyber criminals and its susceptibility to hacking attempts.

In *Home Depot*, this Court allowed a negligence claim premised upon a data breach to continue, noting that the defendant "knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it."[117] Similarly, in *Arby's*, the court noted that the defendant knew about potential data breach threats but failed to implement reasonable security measures.[118] Thus, according to the court, the criminal acts of the cyberhackers were reasonably foreseeable, and thus the plaintiffs' negligence claims could proceed.[119] In *Arby's*, the court compared criminal data breaches to the "peculiarly similar context of premises liability," where the

---

[115] *Arby's*, 2018 WL 2128441, at *4 (quoting *Sturbridge Partners, Ltd. v. Walker*, 267 Ga. 785, 786 (1997)).

[116] *Id.* (quoting *Sturbridge Partners, Ltd.*, 267 Ga. at 786).

[117] *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016).

[118] *Arby's*, 2018 WL 2128441, at *5.

[119] *Id.* at *5-6.

Georgia Supreme Court has held that if a proprietor "has reason to anticipate a criminal act," then he or she has a duty to "exercise ordinary care to guard against injury from dangerous characters."[120]

The Court concludes that, as in *Arby's* and *Home Depot*, the criminal acts of the hackers were reasonably foreseeable to the Defendants, and thus do not insulate them from liability. In the Complaint, the Plaintiffs allege that the Defendants observed major data breaches at other corporations, such as Target, Anthem, and Experian.[121] Equifax itself even experienced prior data breaches.[122] Furthermore, Equifax ignored warnings from cybersecurity experts that its data systems were dangerously deficient, and that there was a substantial risk of an imminent breach.[123] These allegations are sufficient to establish that the acts of the third party cyberhackers were reasonably foreseeable. Thus, the causal chain is not broken.

The Defendants also assert that future identity theft and fraud is a second intervening cause that insulates them from liability.[124] According to the Defendants, the Plaintiffs have not pleaded that this fraudulent conduct is the probable consequence of a data breach, and thus was not foreseeable. However,

---

120 *Id.* at *4 (internal quotations omitted).

121 Consolidated Consumer Class Action Compl. ¶¶ 159-65.

122 *Id.* at ¶¶ 166-82.

123 *Id.* ¶ 179.

124 Defs.' Mot. to Dismiss, at 22-23.

the Court concludes that the Plaintiffs have adequately alleged that such conduct was reasonably foreseeable. In the Complaint, the Plaintiffs allege that the Defendants knew the "likelihood and repercussions" of cybersecurity threats, and had stayed informed as to other well-publicized breaches.[125] The Complaint details the Defendants' alleged awareness of the risks that data breaches pose, including the risks that the compromise of personal information entails.[126] Equifax knew that fraudulent activity had resulted from other, well-publicized data breaches.[127] Thus, the Plaintiffs have adequately alleged that this criminal conduct was reasonably foreseeable.

3. Economic Loss Doctrine

The Defendants next argue that the economic loss doctrine bars the Plaintiffs' tort claims.[128] "The 'economic loss rule' generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort."[129] In other words, "a plaintiff may not recover in tort for purely economic damages arising from a breach of contract."[130] Where,

---

125 Consolidated Consumer Class Action Compl. ¶ 146.

126 *See, e.g.*, *id.* ¶¶ 159-65.

127 *Id.* ¶¶ 160-65.

128 Defs.' Mot. to Dismiss, at 23.

129 *General Elec. Co. v. Lowe's Home Centers, Inc.*, 279 Ga. 77, 78 (2005).

130 *Hanover Ins. Co. v. Hermosa Const. Grp., LLC*, 57 F. Supp. 3d 1389, 1395 (N.D. Ga. 2014).

however, "an independent duty exists under the law, the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule."[131] Here, the independent duty exception would bar application of the economic loss rule. "It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information[.]"[132] As discussed below, the Defendants owed the Plaintiffs a duty of care to safeguard their personal information. Therefore, since an independent duty existed, the economic loss rule does not apply.

D. Negligence

Next, the Defendants move to dismiss the Plaintiffs' negligence claim.[133] In Count 2 of the Complaint, the Plaintiffs allege that Equifax owed a duty to the Plaintiffs to "exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons."[134] The Plaintiffs also allege that Equifax had a duty of care that arose from Section 5 of the Federal Trade Commission Act (the "FTC

---

131 *Liberty Mut. Fire Ins. Co. v. Cagle's, Inc.*, No. 1:10-cv-2158-TWT, 2010 WL 5288673, at *3 (N.D. Ga. Dec. 16, 2010).

132 *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017).

133 Defs.' Mot. to Dismiss, at 24.

134 Consolidated Consumer Class Action Compl. ¶ 334.

Act"), and the FCRA.[135] The Defendants contend that they were under no duty of care toward the Plaintiffs.[136]

In Georgia, "[a] cause of action for negligence requires (1) [a] legal duty to conform to a standard of conduct raised by the law for the protection of others against unreasonable risks of harm; (2) a breach of this standard; (3) a legally attributable causal connection between the conduct and the resulting injury; and, (4) some loss or damage flowing to the plaintiff's legally protected interest as a result of the alleged breach of the legal duty."[137] "The threshold issue in any cause of action for negligence is whether, and to what extent, the defendant owes the plaintiff a duty of care."[138] Whether such a duty exists is a question of law.[139] Georgia recognizes a general duty "to all the world not to subject them to an unreasonable risk of harm."[140]

The Defendants contend that Georgia law does not impose a duty of care

---

135 *Id.* ¶¶ 337, 340.

136 This argument seems more than a little cynical in light of Equifax's public description of itself as the "trusted steward" of consumer data.

137 *Dupree v. Keller Indus.*, Inc., 199 Ga. App. 138, 141 (1991) (internal quotations omitted).

138 *Access Mgmt. Grp., L.P. v. Hanham*, 345 Ga. App. 130, 133 (2018) (internal quotations omitted).

139 *Id.* (internal quotations omitted).

140 *Bradley Center, Inc. v. Wessner*, 250 Ga. 199, 201 (1982).

to safeguard personal information.[141] The Defendants rely primarily upon a recent Georgia Court of Appeals case, *McConnell v. Georgia Department of Labor*.[142] In *McConnell*, the plaintiff filed a class action against the Georgia Department of Labor after one of its employees sent an email to 1,000 Georgians who had applied for unemployment benefits.[143] This email included a spreadsheet with the name, Social Security number, phone number, email address, and age of 4,000 Georgians who had registered for services with the agency.[144] The plaintiff, whose information was disclosed, filed a class action, asserting, among other claims, a claim for negligence.[145]

A brief overview of *McConnell*'s procedural history is helpful in understanding the court's decision in that case. In June 2016, the Georgia Court of Appeals initially rejected the plaintiff's claims.[146] In *McConnell I*, the plaintiff, recognizing that such a duty had not been expressly recognized in Georgia caselaw, contended that such a duty arose from two statutory sources.[147] The

---

141 Defs.' Mot. to Dismiss, at 24.

142 *Id.*

143 *McConnell v. Dep't of Labor (McConnell III)*, 345 Ga. App. 669, 670 (2018).

144 *Id.*

145 *Id.*

146 *McConnell v. Dep't of Labor (McConnell I)*, 337 Ga. App. 457, 462 (2016).

147 *Id.* at 460.

court concluded that neither of these statutory sources gave rise to a duty to safeguard personal information.[148] The court explained that "McConnell's complaint is premised on a duty of care to safeguard personal information that has no source in Georgia statutory law or caselaw and that his complaint therefore failed to state a claim of negligence."[149] However, in doing so, the court expressly distinguished this Court's prior holding in *Home Depot*, noting that this Court "found a duty to protect the personal information of the defendant's customers in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies" and explaining that "[t]here are no such allegations in this case."[150]

Then, the Georgia Supreme Court vacated *McConnell I*, holding that the Court of Appeals could not decide whether the plaintiff failed to state a claim without first considering whether the doctrine of sovereign immunity barred his claims.[151] On remand, the Georgia Court of Appeals, after deciding that sovereign immunity did not bar the plaintiff's claims, once again concluded that

---

148 *Id.* at 461-62.

149 *Id.* at 462.

150 *Id.* at 460 n.4.

151 *McConnell v. Dep't of Labor (McConnell II)*, 302 Ga. 18, 18-19 (2017).

the plaintiff's negligence claim failed because "McConnell's complaint is premised on a duty of care to safeguard personal information that has no source in Georgia statutory law or caselaw and that his complaint therefore failed to state a claim of negligence."[152] Examining both the Georgia Personal Identity Protection Act and the Georgia Fair Business Practices Act, the court concluded that neither gave rise to a duty to safeguard personal information.[153] Although the legislature showed a "concern about the cost of identity theft to the marketplace" through these statutes, it did not act to "establish a standard of conduct intended to protect the security of personal information, as some other jurisdictions have done in connection with data protection and data breach notification laws."[154]

The Defendants contend that *McConnell III* confirms that there is no duty under Georgia law, common law or statutory, to safeguard personally identifiable information.[155] The Georgia Supreme Court has granted certiorari in the case. The Defendants, at oral argument, asked the Court to delay ruling upon the Motion to Dismiss until a ruling by the Georgia Supreme Court. However, it seems very unlikely to me that the Georgia Supreme Court will

---

[152] *McConnell v. Dep't of Labor (McConnell III)*, 345 Ga. App. 669, 678-679 (2018).

[153] *Id.* at 676-79.

[154] *Id.* at 679.

[155] Defs.' Mot. to Dismiss, at 26.

adopt a rule of law that tells hundreds of millions of consumers in the United States that a national credit reporting agency headquartered in Georgia has no obligation to protect their confidential personal identifying data. Unlike the Georgia Department of Labor, Equifax and the other national credit reporting agencies are heavily regulated by federal law. As noted previously, the Fair Credit Reporting Act strictly limits the circumstances under which a credit reporting agency may disclose consumer credit information.[156] The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.[157] The Gramm–Leach–Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information. [158] The FTC has done that.[159]

The Plaintiffs contend that, under Georgia law, allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish a duty of care.[160] The Plaintiffs rely primarily upon *Home Depot* and

---

156 *See* 15 U. S. C. § 1681b(a).

157 Federal Trade Commission Act. 15 U.S.C.A. § 45(a); *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015).

158 *See* 15 U.S.C. § 6801(b).

159 *See* 16 C.F.R. §314.4(b-e).

160 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 9.

Arby's for this proposition. In *Home Depot*, this Court denied the defendant's motion to dismiss a negligence claim arising out of a data breach.[161] The Court concluded that Home Depot had a duty to safeguard customer information because it "knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it."[162] The Court, citing the Georgia Supreme Court's decision in *Bradley Center, Inc. v. Wessner*, came to this conclusion by expounding upon the general duty to "all the world not to subject them to an unreasonable risk of harm."[163] The Court noted that "to hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk."[164]

Then, in *Arby's*, the court declined to dismiss a plaintiff's negligence claim arising out of a data breach. The court explained that "[u]nder Georgia law and the standard articulated in *Home Depot*, allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the

---

[161] *In re The Home Depot, Inc. Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *1 (N.D. Ga. May 18, 2016).

[162] *Id.* at *3.

[163] *Id.* (quoting *Bradley Ctr., Inc. v. Wessner*, 250 Ga. 199, 201 (1982)).

[164] *Id.* at *4.

existence of a plausible legal duty and survive a motion to dismiss."[165] The court held that Arby's was under a duty to safeguard its customers' personal data due to allegations that it knew about potential problems and failed to implement reasonable security measures, knew about other highly-publicized data breaches, and was aware that its parent company had suffered a significant breach using the same computer system.[166] The *Arby's* court also distinguished *McConnell I*, explaining that it was not "expressly inconsistent" with *Home Depot* because *Home Depot* found a duty to protect personal information in the context of the defendant's failure to implement reasonable security measures to combat a foreseeable risk, while there were no such allegations in *McConnell I*.[167] The court also explained that the *McConnell I* court's characterization of *Wessner* as a narrow holding did not change its conclusion since *McConnell I* did not change the general duty that arises from foreseeable criminal acts.[168]

The parties' interpretations of this caselaw diverge greatly. The Defendants contend that *McConnell III*, the latest decision of all of these cases, clarified this caselaw and affirmatively stated that there is no duty to safeguard

---

165 *In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-1035-AT, 2018 WL 2128441, at *5 (N.D. Ga. Mar. 5, 2018).

166 *Id.* at *5.

167 *Id.* at *6.

168 *Id.* at *7.

personal information.[169] Thus, according to the Defendants, *Home Depot* and *Arby's* are no longer good law.[170] The Plaintiffs, in turn, argue that due to the factual differences between *McConnell III*, on the one hand, and *Arby's* and *Home Depot,* on the other hand, *McConnell III* does not conflict with these two cases.[171] According to the Plaintiffs, there were no allegations in *McConnell III* that the state agency should have known that its employee would inadvertently disclose this personal information. In contrast, *Home Depot* and *Arby's* premised their holdings on the detailed allegations that the data breaches were foreseeable.[172] Finally, the Plaintiffs argue that, despite the Defendants' characterizations, they are not asking this Court to recognize a new duty under Georgia law, but instead are asking it to apply traditional tort and negligence principles to the facts of this case.[173]

The Court concludes that, under the facts alleged in the Complaint, Equifax owed the Plaintiffs a duty of care to safeguard the personal information in its custody. This duty of care arises from the allegations that the Defendants knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures. *McConnell III* does not alter this conclusion. As

---

169 Defs.' Mot. to Dismiss, at 29-30.

170 *Id.*

171 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 14-15.

172 *Id.* at 14-15.

173 *Id.* at 16.

the court in *McConnell I* noted, a critical distinction between these cases is that the duty in *Home Depot* arose from allegations that the defendant failed to implement reasonable security measures in the face of a known security risk.[174] Such allegations did not exist in the *McConnell* line of cases.[175] The *McConnell III* court came to the same conclusion as the *McConnell I* court, and did nothing to dispel this distinction made in *McConnell III*. Furthermore, given this mention of *Home Depot* in *McConnell I*, and the court's subsequent holding in *Arby's*, the *McConnell III* court's silence on this issue suggests a tacit approval of this distinction. And, as this Court noted in *Home Depot*, to hold otherwise would create perverse incentives for businesses who profit off of the use of consumers' personal data to turn a blind eye and ignore known security risks.[176]

The Defendants go to great lengths to distinguish the Georgia Supreme Court's decision in *Bradley Center, Inc. v. Wessner.* Both *Home Depot* and *Arby's* relied, in part, upon *Wessner* to conclude that the defendants were under a duty to take reasonable measures to avoid a foreseeable risk of harm from a data breach incident. In *Wessner*, a man who voluntarily committed himself to a psychiatric hospital made statements to the hospital's staff that he desired to harm his wife.[177] Despite these statements, the man was issued a weekend pass

---

174 *McConnell I*, 337 Ga. App. at 461 n.4.

175 *Id.*

176 *See Home Depot*, 2016 WL 2897520, at *4.

177 *Bradley Ctr., Inc. v. Wessner*, 250 Ga. 199, 199-200 (1982).

by the staff, and he subsequently obtained a gun, confronted his wife and another man, and killed them both.[178] The Georgia Supreme Court concluded that the hospital owed a duty of care to the man's wife.[179] The court explained that "[t]he legal duty in this case arises out of the general duty one owes to all the world not to subject them to an unreasonable risk of harm."[180]

The Defendants argue that the holding in *Wessner* is much narrower than this. According to them, *Wessner* merely stands for the narrow proposition that a physician owes a legal duty when, in the course of treating a mental health patient, that physician exercises control over the patient and knows or should know that the patient is likely to cause harm to others. The Defendants further assert that the *Wessner* court's references to general negligence principles were done in an effort to explain why the case was a negligence case, and not a medical malpractice case. However, despite the Defendants' efforts to minimize the importance of *Wessner*, the Court finds that *Wessner* supports the conclusion that the Defendants owed a legal duty to take reasonable measures to prevent a reasonably foreseeable risk of harm due to a data breach incident. Nowhere in the *Wessner* decision does the Georgia Supreme Court limit its holding to the narrow proposition that the Defendants assert. In fact, in

---

178 *Id.* at 200.

179 *Id.* at 200-02.

180 *Id.* at 201.

Wessner, the court explained that it was not creating a "new tort," but instead that it was applying "our traditional tort principles of negligence to the facts of this case."[181] Other Georgia cases have similarly applied these same general principles.[182] Likewise, this Court concludes that, under traditional negligence principles, the Defendants owed a legal duty to the Plaintiffs to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident.

The Defendants then argue that they did not "voluntarily" undertake a duty.[183] In the Complaint, the Plaintiffs allege that Equifax's duty also arose from its "unique position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system" and that Equifax "undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers."[184] The Defendants contend that this claim fails because under Georgia's "good Samaritan" provision, an undertaken duty extends only to preventing physical harm to another's person or property.[185] The Plaintiffs do not respond to this argument. Therefore, to the extent that the Plaintiffs assert

---

181 *Id.* at 202.

182 *See Underwood v. Select Tire, Inc.*, 296 Ga. App. 805, 809 (2009) (describing the general duty one owes to the world to not subject them to an unreasonable risk of harm).

183 Defs.' Mot. to Dismiss, at 32.

184 Consolidated Consumer Class Action Comp. ¶ 338.

185 Defs.' Mot. to Dismiss, at 32.

a duty premised upon the Defendants' voluntary undertaking such a responsibility, that claim should be dismissed.

E. Negligence Per Se

Next, the Defendants move to dismiss the Plaintiffs' negligence per se claim.[186] In Count 3 of the Complaint, the Plaintiffs allege that Equifax violated Section 5 of the FTC Act, and similar state statutes, by "failing to use reasonable measures to protect Personal Information and not complying with industry standards," and that such violation constitutes negligence per se.[187] "Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se."[188] In order to make a negligence per se claim, however, the plaintiff must show that it is within the class of persons intended to be protected by the statute and that the statute was meant to protect against the harm suffered.[189]

The Defendants argue that the Plaintiffs fail to identify statutory text that imposes a duty with specificity upon the Defendants. Here, the Plaintiffs allege that Equifax violated Section 5 of the FTC Act. The Defendants argue that Section 5 cannot form the basis of a negligence per se claim. The failure to

---

186 Defs.' Mot. to Dismiss, at 34.

187 Consolidated Consumer Class Action Compl. ¶¶ 350-51.

188 *Pulte Home v. Simerly*, 322 Ga. App. 699, 705 (2013).

189 *Amick v. BM & KM, Inc.*, 275 F. Supp. 2d 1378, 1382 (N.D. Ga. 2003).

maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.[190] The Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect.[191] Additionally, one Georgia case and one case applying Georgia law both suggest that the FTC Act can serve as the basis of a negligence per se claim.[192] The Defendants' motion to dismiss the negligence per se claim should be denied.

Second, the Defendants argue that *LabMD, Inc. v. Fed. Trade Comm'n,* should lead this Court to a different conclusion.[193] That was a direct enforcement action. There, the Eleventh Circuit noted that "standards of unfairness" must be found "in 'clear and well-established' policies that are expressed in the

---

[190] 15 U.S.C.A. § 45(a); *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015).

[191] *See Arby's*, 2018 WL 2128441, at *8 (concluding that similar allegations were sufficient to plead a violation of Section 5).

[192] *Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360-JCT, 2014 WL 637762, at *13-14 (W.D. Va. Feb. 12, 2014) (applying Georgia law); *Legacy Acad., Inc. v. Mamilove, LLC*, 328 Ga. App. 775, 790 (2014), *aff'd in part and rev'd in part on other grounds*, 297 Ga. 15 (2015).

[193] *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221 (11th Cir. 2018).

Constitution, statutes, or the common law."[194] The court explained that the FTC in that case did "not explicitly cite the source of the standard of unfairness" it used in holding that LabMD's failure to implement a reasonable data security program was an unfair act or practice, but concluded that it was "apparent" that "the source is the common law of negligence." The court then vacated the FTC's order because the order was too vague to be enforced. It did not hold that inadequate data security cannot be regulated under Section 5.

Next, the Defendants argue that the Plaintiffs have not sufficiently alleged injury or proximate causation. Under Georgia law, negligence per se is "not liability per se."[195] Even if negligence per se is shown, a plaintiff must still prove proximate causation and actual damage to recover.[196] As discussed above, the Court concludes that the Plaintiffs have sufficiently alleged both a legally cognizable injury and proximate causation. Therefore, this argument is unavailing.

F. Georgia Fair Business Practices Act

Next, the Defendants move to dismiss the Plaintiffs' claims under the Georgia Fair Business Practices Act. The Georgia Fair Business Practices Act prohibits, generally, "unfair or deceptive acts or practices in the conduct of

---

194 *Id.* at 1231.

195 *Hite v. Anderson*, 284 Ga. App. 156, 158 (2007).

196 *Id.*

consumer transactions and consumer acts or practices in trade or commerce."[197] In Count 4 of the Complaint, the Plaintiffs allege that the Defendants violated multiple provisions of the Georgia Fair Business Practices Act, including O.C.G.A. §§ 10-1-393(a), 10-1-393(b)(5), 10-1-393(b)(7), 10-1-393(b)(9).[198] The Defendants make multiple arguments in favor of dismissal.

The Defendants first argue that the Georgia Fair Business Practices Act does not require the safeguarding of personally identifiable information.[199] According to the Defendants, *McConnell III* would have been decided differently if the Georgia Fair Business Practices Act contained such a requirement.[200] In *McConnell III*, the court concluded that part of the Georgia Fair Business Practices Act, O.C.G.A. § 10-1-393.8, "can not serve as the source of such a general duty to safeguard and protect the personal information of another."[201] That provision prohibited "intentionally communicating a person's social security number."[202] The court rejected the plaintiff's claim, noting that he had alleged that the defendant negligently disseminated his social security

---

197 O.C.G.A. § 10-1-393(a).

198 Consolidated Consumer Class Action Compl. ¶¶ 355-80.

199 Defs.' Mot. to Dismiss, at 38-39.

200 *Id.* at 38.

201 *McConnell v. Dep't of Labor* (*McConnell III*), 345 Ga. App. 669, 678 (2018).

202 *Id.* (emphasis omitted).

number.[203]

The Plaintiffs make multiple arguments in response. However, the Court finds these arguments unpersuasive. First, they argue that *Arby's II*, decided after *McConnell III*, held that data breach victims can pursue a claim under the Georgia Fair Business Practices Act. However, that decision only considered whether the plaintiffs had adequately alleged reliance.[204] Thus, the court's reasoning does not bear on whether *McConnell III* precluded recovery under the Georgia Fair Business Practices Act. Second, the Plaintiffs contend that *McConnell III* only stands for the proposition that the Georgia Fair Business Practices Act is not the basis of a general tort duty. However, *McConnell III*'s holding was broader than that. In *McConnell III*, the court, after examining parts of the Georgia Fair Business Practices Act, along with the Georgia Personal Identity Protection Act, concluded that there is no statutory basis for a duty to safeguard personal information in Georgia.[205] It further explained that the Georgia legislature has not acted to establish a standard of conduct to protect the security of personal information, unlike other jurisdictions with data protection and data breach laws.[206] Even though *McConnell III* examined the

---

[203] *Id.*

[204] *See In re Arby's Restaurant Grp. Inc. Litig.*, 317 F. Supp. 3d 1222, 1224 (N.D. Ga. 2018).

[205] *McConnell III*, 345 Ga. App. 669, 677-79.

[206] *Id.* at 679.

Georgia Fair Business Practices Act in the context of its provisions dealing with Social Security numbers specifically, it concluded that the entire Act, along with the rest of Georgia statutory law, did not require the safeguarding of personal information. Therefore, the Court concludes that the Georgia Fair Business Practices Act does not require businesses to safeguard personally identifiable information. This issue may be revisited depending upon the ruling of the Georgia Supreme Court in *McConnell III*.

G. Unjust Enrichment

The Defendants next move to dismiss the Plaintiffs' unjust enrichment claim. In Count 5 of the Complaint, the Plaintiffs allege that Equifax has been unjustly enriched by benefitting from and profiting off of the sale of the Plaintiffs' personally identifiable information, all at the Plaintiffs' expense.[207] Unjust enrichment is an equitable doctrine that "applies when as a matter of fact there is no legal contract, but where the party sought to be charged has been conferred a benefit by the party contending an unjust enrichment which the benefitted party equitably ought to return or compensate for."[208] Thus, in order to state a claim for unjust enrichment, the Plaintiffs must show that "(1) a benefit has been conferred, (2) compensation has not been given for receipt of

---

[207] Consolidated Consumer Class Action Compl. ¶¶ 382-91.

[208] *Engram v. Engram*, 265 Ga. 804, 806 (1995) (quotations and some punctuation omitted).

the benefit, and (3) the failure to so compensate would be unjust."[209]

The Defendants argue that, with regard to most of the Plaintiffs, personally identifiable information was conferred on Equifax by third parties, and not by the Plaintiffs themselves.[210] Instead, only the Contract Plaintiffs gave their information to Equifax. Thus, according to the Defendants, the unjust enrichment claims of these non-Contract Plaintiffs fail because they do not allege that they conferred anything of value on Equifax.[211]

The Plaintiffs first cite *Arby's*, contending that the court in that case "sustain[ed]" the plaintiffs' claim for unjust enrichment. However, the court in *Arby's* did not consider the merits of the plaintiffs' unjust enrichment claim. Instead, it merely decided that the plaintiffs could assert a claim for unjust enrichment in the alternative to their contract claims.[212] Therefore, this case does not provide guidance as to whether the Plaintiffs have made allegations that satisfy each element of an unjust enrichment claim. The Plaintiffs also cite

---

[209] *Hill v. Clark*, No. 2:11-CV-0057-RWS, 2012 WL 787398, at *6 (N.D. Ga. Mar. 7, 2012).

[210] Defs.' Mot. to Dismiss, at 42.

[211] *Id.*

[212] *See In re Arby's Restaurant Grp. Inc. Litig.*, No. 1:17-cv-0514-AT, 2018 WL 2128441, at *17 (N.D. Ga. Mar. 5, 2018) ("Therefore, the Consumer Plaintiffs are entitled to assert a claim for unjust enrichment in the alternative to their claim for breach of an implied-in-fact contract.").

Sackin v. TransPerfect Global, Inc.[213] However, the plaintiffs in that case asserted an unjust enrichment claim under New York law, which contains different elements than such a claim under Georgia law.[214]

The Court concludes that the non-Contract Plaintiffs fail to establish the necessary elements of an unjust enrichment claim. The Georgia Court of Appeals has explained that "for unjust enrichment to apply, the party conferring the labor and things of value must act with the expectation that the other will be responsible for the cost. Otherwise, that party, like one who volunteers to pay the debt of another, has no right to an equitable recovery."[215] For example, in *Sitterli v. Csachi*, the court concluded that for unjust enrichment to apply, the party conferring things of value must act with the expectation that the other will be responsible for the cost. The Plaintiffs have failed to show that they conferred a thing of value, namely their personally identifiable information, upon the Defendants with the expectation that Equifax would be responsible for

---

[213] *Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739 (S.D.N.Y. 2017).

[214] *See id.* at 751 (quoting *Ga. Malone & Co. v. Rieder*, 973 N.E.2d 743 (2012)) (The plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered.); *see also Engram v. Engram*, 265 Ga. 804, 806 (1995) ("[T]he undisputed evidence shows that the parties never intended that appellees be responsible for the cost of the bedroom addition.").

[215] *Sitterli v. Csachi*, 344 Ga. App. 671, 673 (2018) (internal quotations and alterations omitted).

the cost. The non-Contract Plaintiffs have failed to allege that they had any such expectation.

The Defendants also argue that the Contract Plaintiffs' unjust enrichment claims must be dismissed because those Plaintiffs have also pleaded breach of contract claims.[216] Under Georgia law, "[a] party can only recover for a claim of unjust enrichment if there is not an express contract that governs the dispute."[217] However, "[w]hile a party, indeed, cannot recover under both a breach of contract and unjust enrichment theory, a plaintiff may plead these claims in the alternative."[218] Thus, the Contract Plaintiffs may assert inconsistent contract and unjust enrichment theories at this stage of the proceedings.

H. Breach of Contract

Next, the Defendants move to dismiss the Contract Plaintiffs' breach of contract claims.[219] Nineteen Plaintiffs allege that they formed a contract with Equifax, either express or implied, when they obtained credit monitoring or identity theft protection services from the company.[220] According to these

---

216 Defs.' Mot. to Dismiss, at 42.

217 *Arby's*, 2018 WL 2128441, at *17 (citing *Fed. Ins. Co. v. Westside Supply Co.*, 264 Ga. App. 240, 248 (2003)).

218 *Clark v. Aaron's, Inc.*, 914 F. Supp. 2d 1301, 1309 (N.D. Ga. 2012).

219 Defs.' Mot. to Dismiss, at 44-49.

220 Consolidated Consumer Class Action Compl. ¶¶ 405, 410.

Contract Plaintiffs, Equifax's Privacy Policy constituted an agreement between Equifax and those individuals who provided personal information to it, including the Contract Plaintiffs.[221] Equifax's Privacy Policy states that Equifax "restrict[s] access to personally identifiable information . . . that is collected about you to only those who have a need to know that information in connection with the purpose for which it is collected and used."[222] Equifax allegedly breached this contract by failing to take steps to protect the Contract Plaintiffs' personal information.[223]

The Defendants argue that the Privacy Policy is not a contract, and even if it is, it did not impose the obligations that the Plaintiffs assert.[224] They argue that the Contract Plaintiffs' purchases were governed by an express contract, with a merger clause, that does not incorporate the Privacy Policy.[225] Under Georgia law, "a merger clause operates as a disclaimer of all representations not made on the face of the contract."[226] The Equifax Product Agreement and Terms of Use, which the Defendants contend was the sole contract entered into between Equifax and the Contract Plaintiffs, provides that "[t]his Agreement

---

221 *Id.* ¶ 401.

222 *Id.* ¶ 152.

223 *Id.* ¶ 407.

224 Defs.' Mot. to Dismiss, at 44.

225 *Id.*

226 *Ekeledo v. Amporful*, 281 Ga. 817, 819 (2007).

constitutes the entire agreement between You and Us regarding the Products and information contained on or acquired through this Site or provided by Us."[227] However, even if this is a valid merger clause, the Equifax Terms of Use go on to provide that these terms are "[s]ubject to the conditions described on the privacy page of this Web Site."[228] Therefore, the Court concludes that the merger clause in the Terms of Use does not preclude the Contract Plaintiffs' claims.

The Contract Plaintiffs argue that they adequately pleaded that the Privacy Policy constituted a contract when they purchased services from Equifax, obtained their credit files, disputed their entries, or more.[229] Courts have concluded that a business's privacy policy can constitute a stand-alone contract.[230] However, the Contract Plaintiffs have not explicitly alleged that they read the Privacy Policy, or otherwise relied upon or were aware of the representations and assurances made in the Privacy Policy when choosing to use the Defendants' services. Without such a showing, the Plaintiffs have failed to

---

[227] *See* [Doc. 464-1], at 7.

[228] *Id.* at 8.

[229] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 40-41.

[230] *See, e.g.*, *In re JetBlue Airways Corp. Privacy Lit.*, 379 F. Supp. 2d 299, 325 (E.D.N.Y. 2005) ("Although plaintiffs do allege that the privacy policy constituted a term in the contract of carriage, they argue alternatively that a stand-alone contract was formed at the moment they made flight reservations in reliance on express promises contained in JetBlue's privacy policy. JetBlue posits no persuasive argument why this alternative formulation does not form the basis of a contract.").

establish the essential element of mutual assent.[231] The Plaintiffs also assert that the Product Agreement and Terms of Use incorporated the Privacy Policy.[232] However, even if the Plaintiffs establish that the Privacy Policy was part of this express contract, the terms of the agreement provide that Equifax will not "be liable to any party for any direct, indirect, special or other consequential damages for any use of or reliance upon the information found at this web site."[233] Thus, even assuming the Privacy Policy was incorporated by reference, under the terms of this agreement the Plaintiffs cannot seek damages relating to the information in Equifax's custody.[234]

The Plaintiffs alternatively assert an implied contract claim.[235] However, this claim fails. As discussed above, the Equifax Terms of Use contained a valid merger clause. Such a clause precludes the assertion of an implied contract

---

[231] *See, e.g.*, *id.* at 325 ("JetBlue further argues that failure to allege that plaintiffs read the privacy policy defeats any claim of reliance. Although plaintiffs do not explicitly allege that the class members actually read or saw the privacy policy, they do allege that they and other class members relied on the representations and assurances contained in the privacy policy when choosing to purchase air transportation from JetBlue.").

[232] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 41-42.

[233] *See* [Doc. 464-1], at 7.

[234] Due to the existence of a merger clause, the Contract Plaintiffs' implied contract claims also must necessarily fail.

[235] Consolidated Consumer Class Action Compl. ¶¶ 409-16.

claim.[236] Furthermore, the Plaintiffs have failed to allege facts establishing the necessary elements of an implied contract claim. The Georgia Court of Appeals has explained that, for both express and implied contract claims, "[t]he concept of a contract requires that the minds of the parties shall meet and accord at the same time, upon the same subject matter, and in the same sense."[237] "In the absence of this meeting of the minds, there is no special contractual provisions between the alleged contracting parties."[238] An implied contract only differs from an express contract in the type of proof used to prove its existence.[239] The same element of mutual assent is required.[240] The Contract Plaintiffs allege that an implied contract was formed because "Equifax agreed to safeguard and protect the Personal Information of Plaintiffs and Class members and to timely and accurately notify them if their Personal Information was breached or compromised."[241] This conclusory allegation fails to establish the necessary element of mutual assent. This allegation, which contains a legal conclusion

---

[236] *See Ekeledo v. Amporful*, 281 Ga. 817, 819 (2007) ("In essence, a merger clause operates as a disclaimer of all representations not made on the face of the contract.").

[237] *Donaldson v. Olympic Health Spa, Inc.*, 175 Ga. App. 258, 259 (1985).

[238] *Id.*

[239] *Grange Mut. Cas. Co. v. Woodard*, 300 Ga. 848, 853 (2017).

[240] *Id.*

[241] Consolidated Consumer Class Action Compl. ¶ 411.

instead of a factual allegation, fails to show that the Defendants and the Contract Plaintiffs had a meeting of the minds, as required by Georgia law. Therefore, the Contract Plaintiffs' implied contract claim fails to state a claim.

I. State Statutes

1. State Business Fraud and Consumer Protection Statutes

The Defendants move to dismiss the Plaintiffs' claims under a variety of state business fraud and consumer protection statutes. The Defendants first argue that these statutes cannot apply to conduct that took place entirely in Georgia. Second, they contend that the Plaintiffs have not adequately alleged fraud, scienter, or injury. Third, they contend that the Plaintiffs have failed to establish that they had "consumer transactions," as many statutes require. Fourth, the Defendants assert that the Plaintiffs fail to allege that they were under a duty to disclose. Fifth, the Defendants argue that the Plaintiffs' claims for damages fail under statutes that provide only for equitable relief. Then, the Defendants contend that the Plaintiffs assert many claims under statutes that do not provide a private right of action. Finally, the Defendants contend that the Plaintiffs' claims under the Georgia Uniform Deceptive Trade Practices Act must fail. The Court addresses each of these arguments in turn.

i. Extraterritoriality

The Defendants contend that the deceptive trade practice laws of foreign

states cannot be applied to conduct that took place in Georgia.[242] The Defendants argue that these state statutes do not extend to conduct that occurred in Georgia. In a support of this proposition, they cite authority from eight of these states. However, that authority merely states that the statutes apply in those specific states. They do not stand for the proposition that the statutes only apply to conduct that takes place within those states. These cases also stand for the general proposition that there are limits to the sovereignty of each state, and that there are limits to the reach of those states' laws. They do not, however, stand for the proposition that the laws of these states only extend to conduct that takes place within the states, or that the specific consumer protection statutes asserted by the Plaintiffs only extend to conduct taking place within the states. The Plaintiffs, who allege that they were harmed in each of these respective states, have adequately stated claims under these state statutes.[243]

Second, the Defendants argue that these foreign states lack authority under the Constitution to govern conduct occurring in Georgia.[244] The Defendants cite *State Farm Mutual Automobile Insurance Company v.*

---

[242] Defs.' Mot. to Dismiss, at 53-54.

[243] *See, e.g.*, *McKinnon v. Dollar Thrifty Auto. Grp., Inc.*, No. 12-4457 SC, 2013 WL 791457, at *5 (N.D. Cal. Mar. 4, 2013) ("California residents can bring claims against out-of-state defendants if their injuries occurred in California.").

[244] Defs.' Mot. to Dismiss, at 54.

Campbell.[245] In *State Farm*, the Supreme Court imposed extraterritorial limitations on punitive damages awards.[246] However, the Supreme Court did not hold that states are powerless to regulate out-of-state conduct. Instead, in *State Farm*, the Court held that, in the context of punitive damages, "lawful out-of-state conduct may not be used to punish a defendant" and "unlawful acts committed out of state to *other persons* may not be used to punish a defendant."[247] *State Farm* does not stand for the proposition that, because all of a defendant's conduct occurred outside of a state, that state cannot enforce its laws against that defendant for injuries occurring in that state.[248] The Defendants also stress that most of the Plaintiffs did not have a direct commercial relationship with Equifax, that Equifax stored its data entirely on computers located in Georgia that were serviced by employees in Georgia, and that the Defendants' acts and omissions occurred only in Georgia.[249] However, even assuming that this is true, the Plaintiffs have alleged that these acts that occurred in Georgia resulted in injuries in other states. These out-of-state

---

[245] *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408 (2003).

[246] *Id.* at 421-22.

[247] *Crouch v. Teledyne Cont'l Motors, Inc.*, No. 10-00072-KD-N, 2011 WL 1539854, at *4 (S.D. Ala. April 21, 2011).

[248] *Id.* ("Neither *State Farm* nor *Sand Hill* supports TCM's conclusion that because all of its 'conduct' occurred outside of Kentucky, punitive damages may not be awarded against it.").

[249] Defs.' Mot. to Dismiss, at 55.

injuries fall within the ambit of many of these foreign state statutes.[250] Therefore, this argument is unavailing.

The Defendants also cite *Healy v. Beer Institute, Inc.*[251] There, the Supreme Court concluded that, under the Dormant Commerce Clause, "a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature."[252] However, the central point of this rule is that "a State may not adopt legislation that has the practical effect of establishing a scale of prices for use in other states."[253] The Court explained that "States may not deprive businesses and consumers in other States of whatever competitive advantages they may possess based on the conditions of the local market."[254] Unlike the statutes at issue in *Healy* and most Dormant Commerce Clause cases, the statutes here do not involve "economic protectionism" and do not discriminate against out-of-state commerce. Thus, this limitation does not apply to the

---

[250] *See Hendricks v. Ford Motor Co.*, No. 4:12CV71, 2012 WL 4478308, at *4 (E.D. Tex. Sept. 27, 2012) ("In *Campbell*, however, fundamental to the Supreme Court's decision was that fact that the out-of-state conduct bore no relation to the plaintiff's harm.").

[251] *Healy v. Beer Inst., Inc.*, 491 U.S. 324 (1989).

[252] *Id.* at 336.

[253] *Id.* (internal quotations omitted).

[254] *Id.* at 339 (internal quotations omitted).

statutes here.

The Defendants then argue that, even if a harmful effect was felt outside of Georgia, that effect was the direct and proximate result of an unknown third party's act, not Equifax's act.[255] However, as explained above, Equifax can be held liable, despite the intervening act of the criminal hackers, due to its failure to properly protect the sensitive data in Equifax's custody. Furthermore, the Defendants have not cited any authority for the proposition that they cannot be held liable under any of these state statutes due to the acts of the criminal third parties. Therefore, this argument is unpersuasive.

ii. Pleading Fraud with Particularity

Next, the Defendants contend that the Plaintiffs have failed to plead fraud with particularity with regard to the state statutes.[256] Rule 9(b) requires a complaint to "state with particularity the circumstances constituting fraud."[257] "A complaint satisfies Rule 9(b) if it sets forth precisely what statements or omissions were made in what documents or oral representations, who made the statements, the time and place of the statements, the content of the statements and manner in which they misled the plaintiff, and what benefit the defendant

---

255 Defs.' Mot. to Dismiss, at 55.

256 *Id.* at 56-59.

257 FED. R. CIV. P. 9(b).

gained as a consequence of the fraud."[258] According to the Defendants, the Plaintiffs have alleged claims under many state laws that are subject to these heightened pleading standards, including their claims for deceptive trade practices.[259]

However, the Court concludes that the Plaintiffs' unfair and deceptive trade practices claims are not subject to Rule 9(b)'s heightened pleading standards. Claims are only subject to these heightened pleading standards if they "sound in fraud."[260] "A claim 'sounds in fraud' when a plaintiff alleges 'a unified course of fraudulent conduct and rel[ies] entirely on that course of conduct as the basis of [that] claim.'"[261] In *Federal Trade Commission v. Hornbeam Special Situations, LLC*, the court considered whether Rule 9(b) applied to claims under § 45(a) of the FTC Act.[262] The court noted that, to "sound in fraud," it is not enough that a claim be near enough to fraud, or fraud-like for

---

[258] *In re Theragenics Corp. Sec. Litig.*, 105 F. Supp. 2d 1342, 1348 (N.D. Ga. 2000) (citing *Brooks v. Blue Cross and Blue Shield of Fla., Inc.*, 116 F.3d 1364, 1371 (11th Cir. 1997)).

[259] Defs.' Mot. to Dismiss, at 56-57.

[260] *See In re AFC Enters., Inc. Sec. Litig.*, 348 F. Supp. 2d 1363, 1376 (N.D. Ga. 2004).

[261] *Burgess v. Religious Tech. Ctr., Inc.*, CIV.A. No. 1:13-cv-02217-SCJ, 2014 WL 11281382, at *6 (N.D. Ga. Feb. 19, 2014).

[262] *Fed. Trade Comm'n v. Hornbeam Special Situations, LLC*, 308 F. Supp. 3d 1280, 1286-87 (N.D. Ga. 2018).

Rule 9(b) to apply.[263] In contrast, to "sound in fraud," the elements of the claim must be similar to that of common law fraud, requiring, among other things, proof of scienter, reliance, and injury.[264]

Here, the Defendants have failed to show that the state unfair and deceptive trade practice statutes sound in fraud. They have not shown that the elements of these statutes are similar to the elements of a common law fraud, and they have not shown that the Plaintiffs' theory of recovery rests upon a unified course of fraudulent conduct. Therefore, the Court concludes that the heightened pleading standards of Rule 9(b) do not apply to these particular state statutes.

The Defendants also cite *Crespo v. Coldwell Banker Mortgage* for the proposition that the Rule 9(b) standard should be applied to claims of deceptive trade practices. However, in *Crespo*, the court applied Rule 9(b)'s heightened standards because the plaintiffs claimed that the defendant "engaged in fraud" by using deceptive trade practices.[265] The plaintiffs asserted a fraud claim, and not a claim arising under a deceptive trade practices statute. Thus, this case is distinguishable.

---

263 *Id.* at 1287.

264 *Id.*

265 *Crespo v. Coldwell Banker Mortg.*, 599 F. App'x 868, 873 (11th Cir. 2014).

iii. Scienter and Injury

Then, the Defendants argue that the Plaintiffs have failed to adequately plead scienter as to their state fraud and consumer protection statutes.[266] According to the Defendants, the Plaintiffs repeatedly assert in the Complaint that Equifax "intended to mislead" the Plaintiffs, but provide no specific factual allegations in support of this conclusion. However, the Court finds the Defendants' argument unpersuasive. The Complaint provides a number of factual allegations demonstrating Equifax's knowledge and intent with regard to its cybersecurity. For instance, the Plaintiffs allege that Equifax was aware of the importance of data security and of the previous well-publicized data breaches.[267] It also provides allegations that, despite this knowledge of cybersecurity risks, Equifax sought to capitalize on the increased number of breaches by providing identity theft protection, instead of taking steps to improve deficiencies in its cybersecurity.[268] The Court finds that these allegations are sufficient.

The Defendants also contend that the Plaintiffs have failed to adequately allege injury.[269] However, as explained above, the Plaintiffs have adequately alleged a legally cognizable injury. The Defendants cite one case for the

---

266 Defs.' Mot. to Dismiss, at 59-60.

267 Consolidated Consumer Class Action Compl. ¶ 159.

268 *Id.* ¶¶ 146-49.

269 Defs.' Mot. to Dismiss, at 60.

proposition that "numerous" state statutes require that an injury be "ascertainable and monetary." However, the Court concludes that the Plaintiffs have largely asserted claims that are ascertainable and monetary. The vast majority of Plaintiffs assert that they spent money taking steps to guard their identity. Furthermore, the Plaintiffs who have alleged that they were victims of identity fraud also allege injuries that are ascertainable and monetary. And, to the extent that any Plaintiffs do not plead injuries that are clearly ascertainable and monetary, the Court concludes that those claims should not be dismissed. As the Plaintiffs emphasize, this requirement comes from one District Court case in California, which has been rejected by numerous other District Courts.[270]

Next, the Defendants contend that the Plaintiffs' claims under state consumer protection statutes requiring "consumer transactions" fail because the non-Contract Plaintiffs do not allege that they engaged in a consumer transaction with Equifax.[271] Although many of these state statutes provide that unfair or deceptive conduct must be done in connection with a consumer transaction, courts have interpreted these requirements liberally.[272] Courts have concluded variously that some of these statutes do not require privity, that some

---

[270] *See, e.g.*, *Corona v. Sony Pictures Entertainment, Inc.*, No. 14–CV–09600 RGK (Ex), 2015 WL 3916744, at *3-4 (C.D. Cal. June 15,2015).

[271] Defs.' Mot. to Dismiss, at 61-62.

[272] *See* Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, Ex. B [Doc. 452-2].

of them do not require a plaintiff to be a direct purchaser of a consumer good, or that the "consumer transaction" language in some of the statutes do not actually impose a requirement for plaintiffs to meet.[273] Therefore, the Court concludes that the state unfair and deceptive trade practices claims under statutes including "consumer transaction" language should not be dismissed.

iv. Duty to Disclose

Next, the Defendants contend that seventeen of the state consumer-fraud statutes do not impose liability for omissions unless there was a duty to disclose.[274] The Court agrees. "In the absence of a confidential relationship, no duty to disclose exists when parties are engaged in arm's-length business negotiations; in fact, an arm's-length relationship by its nature excludes a confidential relationship."[275] The Plaintiffs contend that Equifax was under a duty to disclose due to statements it voluntarily made touting its cybersecurity.[276] However, the vast majority of the Plaintiffs do not even allege that they were in an arms-length transaction with Equifax. Instead, most of the Plaintiffs had no relationship with Equifax. Absent such a relationship, even with these statements touting its cybersecurity, Equifax was under no general

---

[273] *Id.*

[274] Defs.' Mot. to Dismiss, at 63.

[275] *Infrasource, Inc. v. Hahn Yalena Corp.*, 272 Ga. App. 703, 705 (2005).

[276] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 58-59.

duty to disclose to the entire world.

v. Equitable Relief

Next, the Defendants contend that the Plaintiffs seek money damages under four statutes that only provide for injunctive relief.[277] According to the Defendants, the Plaintiffs cannot seek monetary damages under the Illinois, Maine, Minnesota, and Nebraska statutes. The Plaintiffs concede that they do not seek monetary damages under the Maine, Minnesota, and Nebraska Uniform Trade Secrets Acts.[278] The Plaintiffs contend, however, that violation of the Illinois Personal Information Protection Act constitutes a violation of the Illinois Consumer Fraud and Deceptive Trade Practices Act, which expressly permits damages suits.[279] The Court agrees. Since the Illinois Consumer Fraud and Deceptive Trade Practices Act allows for monetary damages, the Plaintiffs' claims for violation of the Personal Information Protection Act can also seek recovery of monetary damages.[280]

---

[277] Defs.' Mot. to Dismiss, at 63.

[278] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 60. They note that they seek all relief allowed by law, including attorneys' fees, which are available under each statute. *Id.*

[279] *Id.*

[280] *See* 815 ILCS § 505-10a(a). In *Allen v. Woodfield Chevrolet, Inc.*, the Supreme Court of Illinois declared amendments to this statute unconstitutional under the Illinois Constitution. *See Allen v. Woodfield Chevrolet, Inc.*, 802 N.E.2d 752, 764-65 (Ill. 2003). These amendments "changed the substantive and procedural requirements for consumer fraud claims against a single group of defendants, namely, new and used vehicle dealers." *Id.* at 756. The court concluded that these amendments violated the Illinois Constitution's

vi. Private Rights of Action

Finally, the Defendants contend that some of the Plaintiffs' claims arise under laws that do not provide a private right of action. Specifically, the Defendants contend that the Massachusetts Consumer Protection Act and the Nevada Deceptive Trade Practices Act do not provide for private rights of action. However, the Court finds these arguments unpersuasive. Both the Massachusetts statute[281] and the Nevada statute[282] are privately enforceable. Therefore, these claims should not be dismissed.

vii. Georgia Uniform Deceptive Trade Practices Act

The Defendants next argue that the Plaintiffs' claims under the Georgia Uniform Deceptive Trade Practices Act, in Count 27, must fail for the same reason that their claims under the Georgia Fair Business Practices Act also fail. The Court agrees. In *McConnell III*, the Georgia Court of Appeals concluded that there is no statutory basis under Georgia law for a duty to safeguard personal information.

---

prohibition against special legislation. *Id.* at 759-760. However, it noted that its decision left intact the rights provided for by the statute prior to this legislation, including a private right of action. *See id.* at 765 ("The effect of our determination is to relegate the parties to such rights as they may have had prior to the enactment of this legislation.").

[281] *See In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009).

[282] *See* N.R.S. § 41.600(1).

2. State Data Breach Notification Statutes

Next, the Defendants move to dismiss the Plaintiffs' claims under state data breach notification statutes.[283] The Defendants contend that twelve of the data breach statutes under which the Plaintiffs assert claims do not allow private rights of action.[284] According to the Defendants, the data breach statutes of Colorado, Delaware, Florida, Iowa, Kansas, Maryland, Michigan, Montana, New Jersey, New York, Wisconsin, and Wyoming do not permit private actions, and the Georgia statute is silent as to whether a private right of action exists.[285]

The Plaintiffs contend that, with regard to the statutes of Iowa, Michigan, and New York, this argument ignores the statutory language.[286] According to the Plaintiffs, courts have interpreted these statutes to be ambiguous as to this question, or that they provide non-exclusive remedies. Iowa's data-breach statute provides that "[a] violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, the attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the

---

283 Defs.' Mot. to Dismiss, at 65.

284 Defs.' Mot. to Dismiss, at 65.

285 *Id.*

286 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 62.

violation."[287] However, it further provides that "[t]he rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law."[288] In *Target*, the court concluded that "[t]his is at least ambiguous as to whether private enforcement is permissible," and thus the Iowa claims should not be dismissed.[289] The Defendants contend that this Court should not follow *Target* where its reasoning is "plainly and persuasively contradicted by other courts or the statutes themselves."[290] However, the Defendants have provided no cases contradicting this reasoning, and the *Target* holding is not inconsistent with the language of the statute. Therefore, this Court likewise concludes that the Plaintiffs' claims under the Iowa data-breach statute should not be dismissed for this reason.

Similarly, Michigan's data-breach statute provides that "a person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice" and that "[t]he attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section."[291]

---

287 IOWA CODE § 715C.2.(9)(a).

288 *Id.* § 715C.2(9)(b).

289 *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014).

290 Defs.' Reply Br., at 34.

291 Mich. Comp. Laws § 445.72(13).

However, this statute also provides that "Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law."[292] In *Target*, the court concluded that this "implies that consumers may bring a civil action to enforce Michigan's data-breach notice statute through Michigan's consumer-protection statute or other laws," and thus this "claim will not be dismissed."[293] Absent any compelling reasoning to the contrary provided by the Defendants, the Court agrees with the *Target* court. The Plaintiffs' claims under the Michigan data-breach statute should not be dismissed due to a lack of a private right of action.

Next, New York's statute provides that "whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation."[294] The statute also provides that "the remedies provided by this section shall be in addition to any other lawful remedy available."[295] At first glance, these claims should survive for the same reasons the Iowa and Michigan claims survived in *Target*. However, this statute also provides that "[t]he provisions of this section shall be exclusive

---

292 *Id.* § 445.72(15).

293 *Target*, 66 F. Supp. 3d at 1169.

294 N.Y. GEN. BUS. LAW § 899-aa(6)(a).

295 *Id.* § 899-aa(6)(b).

and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section."[296] A New York state court interpreted this provision to preclude a private action, reasoning that the "language . . . militates against any implied private right of action" because it would be inconsistent with the legislative scheme.[297] The Court agrees with this reasoning. Thus, since no private right of action exists under New York's data-breach statute, the Plaintiffs' claims under section 899-aa should be dismissed.

The Plaintiffs then contend that four of the data-breach statutes, those of Connecticut, Maryland, Montana, and New Jersey, are enforceable through those states' consumer-protection statutes, even though the data-breach statutes themselves do not contain a private right of action.[298] The Plaintiffs contend that violation of Connecticut's data-breach statute constitutes an unfair trade practice enforceable through its unfair trade practices statute. However, section 36a-701b explicitly states that "[f]ailure to comply with the requirements of this section shall constitute an unfair trade practices for purposes of section 42-110b *and shall be enforced by the Attorney General*."[299] The Plaintiffs, in their brief,

---

296 *Id.* § 899-aa(9).

297 *See Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 19 N.Y.S.3d 850, 858 (N.Y. Sup. Ct. 2015).

298 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 63.

299 CONN. GEN. STAT. § 36a-701b(g) (emphasis added).

conspicuously omit the last part of this provision, which explicitly limits enforcement to the Attorney General. Thus, the Plaintiffs' claims under section 36a-701b should be dismissed.[300] Similarly, the Maryland and Montana data breach statutes are also privately enforceable through those states' unfair trade practices statutes.[301]

The Court similarly concludes that New Jersey's statute provides a private right of action. New Jersey's data breach statute requires any business that conducts business in the state to "disclose any breach of security of . . . computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."[302] The language of the statute does not explicitly allow for a private right of action. The Defendants cite *Holmes v. Countrywide Financial Corp.*, where the court concluded that "[i]nsofar as the Court can tell, § 56:8–163 does not provide a

---

[300] *See Target*, 66 F. Supp. 3d at 1168 (concluding that the language of § 36a–701b(g) "clearly limits enforcement power to the state's attorney general").

[301] *See* MD. CODE ANN. COM. LAW § 14-3508 (noting that a violation of the Maryland Personal Information Protection Act constitutes "an unfair or deceptive trade practice within the meaning of Title 13 of this article"); Mont. Code Ann. § 30-14-1705(3) (providing that "[a] violation of this part is a violation of 30-14-103"); *id.* § 30-14-133(1) (providing that a consumer suffering a loss under § 30-14-103 may bring an individual action).

[302] *See* N.J. STAT. ANN. § 56:8-163.

private right of action for citizens to enforce its provisions."[303] The Plaintiffs respond that violation of this notification statute is considered an unfair trade practice and thus can be privately enforced through the state's consumer protection statute.[304] The Court agrees. Section 56:8-166 provides that violation of such a statute constitutes an unfair trade practice. Thus, this statute provides for a private right of action.

Furthermore, the data breach statutes of Colorado, Delaware, Kansas, and Wyoming contain ambiguous language as to private enforceability or provide that the statute's remedies are "non-exclusive."[305] In *Target*, the court noted that this permissive language is "at least ambiguous as to whether there is a private right of action" and concluded that, "absent any authority construing this ambiguity to exclude private rights of action," the claims should not be

---

[303] *Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205, 2012 WL 2873892, at *13 (W.D. Ky. July 12, 2012).

[304] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 63.

[305] *See* COLO. REV. STAT. § 6-1-716(4) (providing that "[t]he attorney general may bring an action in law or equity to address violations of this section" and that "[t]he provisions of this section are not exclusive"); DEL. CODE ANN. tit. 6 § 12B-104(a) (providing that "the Attorney General may bring an action in law or equity to address the violations of this chapter" and that "[t]he provisions of this chapter are not exclusive"); KAN. STAT. ANN. § 50-7a02(g) (providing that "the attorney general is empowered to bring an action in law or equity to address violations of this section" and that "[t]he provisions of this section are not exclusive"); Wyo. Stat. Ann. § 40-12-502(f) (providing that "[t]he attorney general may bring an action in law or equity to address any violation of this section" and that "[t]he provisions of this section are not exclusive").

dismissed.[306] The Court finds this reasoning persuasive. The Defendants have not identified any authority construing this language as precluding private rights of action. Absent such authority, the Court declines to dismiss the Plaintiffs' claims under the Colorado, Delaware, Kansas, and Wyoming data breach statutes.

Next, the parties disagree as to the Wisconsin data-breach statute. The Defendants contend that the statute does not permit suit by a private plaintiff, while the Plaintiffs contend that the statute is silent. The Court agrees that the statute is silent as to this question. The provision that the Defendants cite, section 134.98(4), provides that "[f]ailure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty."[307] This language does not prohibit a private action. Thus, the Court must decide whether this silence precludes, or supports, a private right of action. Neither party cites authority answering this question. The Plaintiffs cite *Target*, where the court allowed a claim under this statute to survive because neither party cited a case regarding how to interpret silence as to enforcement under Wisconsin law.[308] The court concluded that, absent any

---

306 *See Target*, 66 F. Supp. 3d at 1169.

307 WIS. STAT. § 134.98(4).

308 *Target*, 66 F. Supp. 3d at 1170. In *Target*, the court noted that Wisconsin's statute, like Georgia's, is silent on enforcement, and that it should not be dismissed.

such authority, the plaintiffs' claim should survive. Likewise, the Court here concludes that, without any authority suggesting otherwise, this claim should survive.

Finally, Georgia's statute is silent as to whether a private right of action exists.[309] According to the Defendants, this silence means that a private right of action does not exist. The Defendants, in support of this argument, cite *State Farm Mutual Automobile Insurance Company v. Hernandez Auto Painting and Body Works, Inc.*[310] There, the court noted that the absence of language creating a private right of action "strongly indicates the legislature's intention that no such cause of action be created by said statute."[311] The Court agrees that the absence of any such language in O.C.G.A. § 10-1-912 counsels strongly against inferring a private right of action under Georgia law.[312] *Target* is not persuasive. There, the court concluded that the plaintiffs' claims under section 10-1-912 should survive because "neither party cite[d] any case regarding how a court should interpret silence as to enforcement under Georgia law, and absent any such authority, Plaintiffs have plausibly alleged that private enforcement is

---

309 *See* O.C.G.A. § 10-1-912.

310 Defs.' Mot. to Dismiss, at 65.

311 *State Farm Mut. Auto. Ins. Co. v. Hernandez Auto Painting & Body Works, Inc.*, 312 Ga. App. 756, 761 (2011) (internal quotations omitted).

312 *See id.*; *see also Cross v. Tokio Marine & Fire Ins. Co. Ltd.*, 254 Ga. App. 739, 741 (2002) ("[T]he absence of language in OCGA § 33-3-28 creating a private right of action 'strongly indicates the legislature's intention that no such cause of action be created by said statute.'").

possible and their Georgia claim survives."[313] Here, the Defendants cite Georgia authority to support the proposition that such silence suggests no private right of action exists.[314] Therefore, the claims under O.C.G.A. § 10-1-912 should be dismissed.

Next, the Defendants argue that the Plaintiffs have failed to adequately allege a violation of any of the state data breach notification statutes.[315] According to the Defendants, the Complaint alleges that 41 days elapsed between Equifax's discovery of the Data Breach and the disclosure of the incident to the public.[316] The Defendants contend these state data-breach statutes permit an entity time to determine the scope of a breach before notification, and several of the statutes even establish specific time limits. Therefore, according to the Defendants, their notification met the requirements of these statutes.

However, the Court concludes that the Plaintiffs have adequately alleged a violation of many of these statutes. Theses statutes require notification, for

---

313 *Target*, 66 F. Supp. 3d at 1170.

314 The Plaintiffs also argue that *Hernandez Auto Painting* is not relevant here because it deals with the Georgia Insurance Commissioner's enforcement authority, and does not address the question here. Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 64. However, the reasoning of that case is not limited to the specific statute at issue there. Instead, the court there addressed how to read silence as to the question of a private right of action in general. *See Hernandez Auto Painting*, 312 Ga. App. at 761.

315 Defs.' Mot. to Dismiss, at 66.

316 *Id.* at 66-67.

example, in "the most expedient time possible and without unreasonable delay" and, for example, within a reasonable time.[317] The Plaintiffs have alleged facts from which a jury could conclude that the Defendants did not provide notice within a reasonable time, as these notification statutes require. Therefore, the Court concludes that the Plaintiffs have adequately stated a claim.

The Defendants next argue that the Plaintiffs have failed to adequately allege a claim under the Maryland Social Security Number Privacy Act. This statute prohibits publicly posting or displaying an individual's Social Security number, requiring the individual to transmit his or her Social Security number over the internet unless the connection is secure, initiating the transmission of an individual's Social Security number over the internet unless the connection is secure, and more.[318] In Count 47 of the Complaint, the Plaintiffs allege that the Defendants violated the Maryland Social Security Number Privacy Act by "transmitt[ing] Plaintiff's and Maryland Subclass members' Social Security numbers over the Internet on unsecure connections and/or without encrypting the Social Security Numbers."[319] According to the Defendants, these allegations fail to state a claim because they do not establish that Equifax "initiated" the transmission of any of the Plaintiffs' Social Security numbers over the

---

317 *See, e.g.*, Cal. Civ. Code § 1798.82(a); C.G.S.A. § 36a-701b(b)(1).

318 MD. CODE ANN., Com. Law § 14-3402(a).

319 Consolidated Consumer Class Action Compl. ¶ 824.

internet.[320] The Court agrees. The Plaintiffs, analogizing their arguments under the FCRA, argue that Equifax's conduct was so egregious that it was essentially an active participant in initiating the transmission of the Plaintiffs' Social Security numbers. However, by suffering a criminal hack, the Defendants did not "initiate" the transmission of these Social Security numbers. While the Defendants may have been negligent, the Plaintiffs have not shown that they "initiated the transmission" of their Social Security numbers, or engaged in any other conduct prohibit by this statute. Therefore, this claim should be dismissed.

Finally, the Defendants contend that the Plaintiffs have failed to allege any injury resulting from a delay in notification.[321] According to the Defendants, the Plaintiffs have not alleged when any injury occurred, and thus have not alleged any damage occurring between the time that Equifax should have notified them of the Data Breach, and the time that Equifax did publicly disclose the Data Breach.[322] However, the *Target* court rejected this exact argument. There, the court reasoned that such an argument is premature at this stage and that plaintiffs need only plead "a 'short and plain statement' of their claims" under Rule 8.[323] The Plaintiffs note that they could have frozen their credit

---

320 Defs.' Mot. to Dismiss, at 68.

321 Defs.' Mot. to Dismiss, at 68.

322 *Id.*

323 *Target*, 66 F. Supp. 3d at 1166.

earlier, or taken other precautions.[324] At this stage of the litigation, such allegations are sufficient.

3. "Non-Existent" Plaintiffs

Next, the Defendants contend that the Plaintiffs' claims under the laws of Puerto Rico and the Virgin Islands must be dismissed because no Plaintiff has alleged any connection to, or residence in, either of these territories.[325] However, the Court concludes that the Plaintiffs have adequately alleged claims under Puerto Rico and Virgin Islands law. At this stage of the litigation, it is sufficient to allege that individuals nationwide, including individuals in Puerto Rico and the Virgin Islands, suffered injury from the Data Breach. In *Target*, the court came to the same conclusion, noting that the plaintiffs only need to plausibly allege "that they have standing to represent a class of individuals in every state and the District of Columbia, and thus that they have standing to raise state-law claims in those jurisdictions."[326] The court explained that:

> As Target undoubtedly knows, there are consumers in Delaware, Maine, Rhode Island, Wyoming, and the District of Columbia whose personal financial information was stolen in the 2013 breach. To force Plaintiffs' attorneys to search out those individuals at this stage serves no useful purpose. In this case, and under the specific facts presented here, the Article III standing analysis is best left to after the class-certification stage. Should a

---

[324] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 66.

[325] Defs.' Mot. to Dismiss, at 69.

[326] *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014).

> class be certified, and should that class as certified contain no members from certain states, Target may renew its arguments regarding standing.[327]

Likewise, the Plaintiffs have alleged, and it is very likely, that there are consumers in Puerto Rico and the Virgin Islands whose personal information was compromised in the Data Breach. *Griffin v. Dugger*, cited by the Defendants, is distinguishable because that decision was made in the context of class certification, where such questions are most appropriate.[328] Thus, at this stage, the Plaintiffs have adequately alleged a claim under the laws of these territories.[329]

4. O.C.G.A. § 13-6-11

Finally, the Defendants move to dismiss the Consumer Plaintiffs' claims under O.C.G.A. § 13-6-11. This statute provides that:

> The expenses of litigation generally shall not be allowed as a part of the damages; but where the plaintiff has specially pleaded and has made prayer therefor and where the defendant has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense, the jury may allow them.[330]

---

[327] *Id.*

[328] *See Griffin v. Dugger*, 823 F.2d 1476, 1483 (11th Cir. 1987).

[329] *Target*, 66 F. Supp. 3d at 1160; *see also Langan v. Johnson & Johnson Consumer Cos.*, 897 F.3d 88, 93-96 (2d Cir. 2018) (noting that variations between class members' claims are "substantive questions, not jurisdictional ones" and concluding that differences between state laws are questions of predominance for class certification, and not standing under Article III).

[330] O.C.G.A. § 13-6-11.

The Consumer Plaintiffs contend that they are entitled to recovery under section 13-6-11 because they have plausibly alleged that "Equifax's conduct leading up to the breach was egregious and that both the breach and injury were foreseeable."[331] The Defendants argue that this claim should be dismissed because there is a bona fide controversy or dispute between the parties, and because the Plaintiffs have pleaded no facts suggesting bad faith.[332]

The Plaintiffs do not appear to seek attorneys' fees based upon stubborn litigiousness or unnecessary trouble or extent. Thus, the basis for their claim must be under the "bad faith prong" of section 13-6-11.[333] "'Bad faith' is 'bad faith connected with the transaction and dealings out of which the cause of action arose, rather than bad faith in defending or resisting the claim after the cause of action has already arisen.'"[334] "Bad faith requires more than 'bad judgment' or 'negligence,' rather the statute imports a 'dishonest purpose' or some 'moral obliquity' and implies 'conscious doing of wrong' and a 'breach of known duty through some motive of interest of ill will.'" The Court concludes that the Plaintiffs have alleged facts supporting bad faith. In the Complaint, the

---

331 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 69.

332 Defs.' Mot. to Dismiss, at 69-70.

333 *Lewis v. D. Hays Trucking, Inc.*, 701 F. Supp. 2d 1300, 1313 (N.D. Ga. 2010) ("Plaintiff does not appear to seek any attorney's fees based on resistance of the claim after the cause of action had arisen. Therefore, the basis for Plaintiff's claim must be under the 'bad faith' prong of § 13–6–11.").

334 *Id.*

Plaintiffs have alleged that the Defendants knew of severe deficiencies in their cybersecurity, and of serious threats, but nonetheless declined to act. Based upon Georgia caselaw, the Court concludes that these allegations are sufficient for a claim of bad faith under section 13-6-11.

IV. Conclusion

For the reasons stated above, the Defendants' Motion to Dismiss the Consolidated Consumer Class Action Complaint [Doc. 425] is GRANTED in part and DENIED in part.

SO ORDERED, this 28 day of January, 2019.

/s/Thomas W. Thrash
THOMAS W. THRASH, JR.
United States District Judge