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 FINANCIAL INSTITUTION CASES

OPINION AND ORDER

This is a data breach case. It is before the Court on the Defendants' Motion to Dismiss the Financial Institutions' Consolidated Amended Complaint [Doc. 435]. For the reasons set forth below, the Defendants' Motion to Dismiss the Financial Institutions' Consolidated Amended Complaint [Doc. 435] 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 information of nearly 150 million Americans (the "Data Breach").[2] This personally identifiable information included names, Social Security numbers, birth dates, addresses, driver's license numbers, images of taxpayer ID cards and passports,

---

[1] Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 3, 166 [Doc. 390].

[2] *Id.*

photographs associated with government-issued identification, payment card information, and more.[3] This Data Breach, according to the Plaintiffs, was the direct result of Equifax's disregard for cybersecurity.

Equifax is a Georgia corporation with its principal place of business in Atlanta, Georgia.[4] The Defendant Equifax Information Services LLC is a wholly-owned subsidiary of Equifax with its principal place of business in Atlanta, Georgia.[5] Equifax Information Services collects and reports consumer information to financial institutions, including the Plaintiffs.[6] The Plaintiffs are financial institutions that provide a range of financial services.[7] The Plaintiffs depend greatly on the services provided by Equifax and other credit reporting agencies, since the information they provide is necessary to determine the credit-worthiness of their customers.[8]

According to the Plaintiffs, the Data Breach was the direct result of Equifax's refusal to take the necessary steps to protect the personally identifiable information in its custody. Equifax was warned on numerous occasions that its cybersecurity was dangerously deficient, and that it was

---

[3] *Id.* ¶ 3.

[4] *Id.* ¶ 86.

[5] *Id.* ¶ 87.

[6] *Id.*

[7] *Id.* ¶¶ 12-85.

[8] *Id.* ¶ 97.

vulnerable to data theft and security breaches.[9] In fact, Equifax had suffered multiple security breaches in the past, showing that the Data Breach was not an isolated incident.[10] However, despite these warnings, Equifax did not take the necessary steps to improve its data security or prepare for the known cybersecurity risks.[11]

On March 7, 2017, a vulnerability in the Apache Struts software, a popular open source software program, was discovered.[12] Equifax used Apache Struts to run a dispute portal website.[13] The same day that this vulnerability was announced, the Apache Foundation made available various patches to protect against this vulnerability.[14] The Apache Foundation, along with the U.S. Department of Homeland Security, issued public warnings regarding the vulnerability and the need to implement these patches.[15] Equifax received these warnings and disseminated them internally, but failed to implement the patch.[16] Then, between May 13 and July 30, 2017, hackers exploited this vulnerability

---

9 *Id.* ¶¶ 158-64.

10 *Id.* ¶¶ 150-58.

11 *Id.* ¶¶ 158-64.

12 *Id.* ¶ 176.

13 *Id.* ¶ 173.

14 *Id.* ¶ 177.

15 *Id.* ¶¶ 176-77.

16 *Id.* ¶¶ 179-80.

to enter Equifax's systems.[17] These hackers were able to access multiple databases and exfiltrate sensitive personal information in Equifax's custody.[18] In addition to obtaining this personal information, the hackers accessed 209,000 consumer credit card numbers.[19] On July 29, 2017, Equifax discovered the Data Breach.[20] Equifax's CEO, Richard Smith, was informed of the breach on July 31, 2017.[21] On September 7, 2017, Equifax publicly announced that the Data Breach had occurred.[22]

The Plaintiffs allege that the Data Breach undermined the credit reporting and verification system by exposing this personally identifiable information.[23] According to the Plaintiffs, they were harmed because the Data Breach had a significant impact on financial institutions, including the measures they use to authenticate their customers.[24] The Plaintiffs were forced to expend resources to assess the impact of the Data Breach and their ability to

---

17 *Id.* ¶ 184.

18 *Id.*

19 *Id.* ¶ 186.

20 *Id.* ¶ 196.

21 *Id.* ¶ 198.

22 *Id.* ¶ 203.

23 *Id.* ¶¶ 105-06.

24 *Id.* ¶ 246.

authenticate customers and detect fraud.[25] They have also expended resources establishing new monitoring methods for preventing fraud and will continue to incur costs to develop new modes of preventing such activity.[26] Twenty-three of the Plaintiffs also allege that they issued payment cards that were compromised in the Data Breach.[27] The Plaintiffs assert claims for negligence, negligence per se, negligent misrepresentation, and claims under various state business practices statutes. The Defendants now move to dismiss.

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 requirements to determine the appropriate rules of decision.[28] 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 necessary to make an actor liable for the alleged tort.[29] Usually, this means that the "law of the place of the injury governs rather than the law

---

[25] *Id.* ¶¶ 247-48.

[26] *Id.* ¶ 251.

[27] *See id.* ¶¶ 13-14, 17, 20, 23, 25, 31-33, 36, 39, 44-52, 54-56.

[28] *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.").

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

of the place of the tortious acts allegedly causing the injury."[30] 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."[31] The Plaintiffs identify no foreign statutes that govern their common law claims, therefore the Court will apply Georgia common law.

B. Standing

1. The Financial Institutions

The Defendants contend that the Plaintiffs lack Article III standing.[32] In order to establish standing under Article III, a plaintiff must show an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[33] The Supreme Court has held that "threatened injury must be *certainly impending* to constitute

---

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

[31] *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.").

[32] Defs.' Mot. to Dismiss, at 13.

[33] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013).

injury in fact, and that allegations of *possible* future injury are not sufficient."[34] The Supreme Court has also noted, however, that standing can be "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[35]

First, the Defendants contend that the Plaintiffs' allegations fail because they have failed to make individualized allegations as to standing, and instead assert generic allegations as to the entire putative class.[36] The Plaintiffs have each explained the steps they took after the Data Breach, and the harm that they suffered as a result of the Data Breach.[37] The allegations fall into two groups. The first group of Plaintiffs ("Financial Institutions") allege: (1) they have already spent time and money responding to the compromise of the credit reporting system and personal information they rely upon for their businesses; (2) they have already spent time and money assessing the impact of the Data Breach as required by federal law; and (3) each Plaintiff has already spent time and money mitigating a "substantial risk" of future fraudulent activity.[38] The second group of Plaintiffs ("Financial Institution Card Issuers") make the same allegations plus a fourth: these Plaintiffs issued payment cards compromised

---

[34] *Id.*

[35] *Id.* at 1150 n.5.

[36] Defs.' Mot. to Dismiss, at 14.

[37] *See* Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 12-85.

[38] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 10-11.

in the Data Breach, and have spent time and money reissuing payment cards or reimbursing customers. For each group, the allegations are pretty much word for word the same for each of the Plaintiffs. This is a factor that weighs against finding that the allegations are concrete and particularized. Instead, they are abstract and generalized.

Next, the Defendants contend that the Plaintiffs have not provided sufficient factual allegations demonstrating a cognizable injury-in-fact. A "plaintiff must allege that he has suffered a 'concrete' injury particular to himself."[39] This injury must be "actual or imminent, not conjectural or hypothetical."[40] The Defendants contend that the Plaintiffs' alleged injuries are speculative and conjectural because their "primary theory of harm is focused on actions they might take or costs they may incur due to the theft of consumers' PII" and based on what criminal third party actors might do in the future.[41] According to the Defendants, the Plaintiffs have not identified any customers who were actually affected by the Data Breach, and that they cannot manufacture standing by taking unnecessary steps to protect themselves.[42]

Here, the Plaintiffs have adequately pleaded standing as to the Financial Institution Card Issuers with respect to reissuing payment cards and

---

39 *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1552 (2016).

40 *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

41 Defs.' Mot. to Dismiss, at 15 (emphasis omitted).

42 *Id.* at 16.

reimbursing customers for fraudulent charges. Although the allegations are generalized, the injuries themselves are sufficiently concrete and particularized that they should be easily ascertainable. Specifically, the banks have pleaded actual injury in the form of costs to investigate fraudulent charges, costs to cancel and reissue cards compromised in the data breach, and costs to refund fraudulent charges.[43] These injuries are not speculative and are not threatened future injuries, but are actual, current, monetary damages. The disclosure of payment card numbers is regulated by the Fair Credit Reporting Act.[44] Here, the Financial Institution Card Issuers have adequately pleaded standing.[45] Therefore, the Motion to Dismiss is denied as to these 23 Plaintiffs as to these specific claims.

All of the Financial Institution Plaintiffs allege that they "rel[y] on the accuracy and integrity of the information supplied by the credit reporting system, a reliance which is entirely foreseeable by Equifax, given the role that

---

[43] Financial Institution Pls.' Consolidated Class Action Compl. ¶¶ 8-10, 105-06, 230-249.

[44] 15 U. S. C. § 1681c(g).

[45] *See 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) ("Specifically, the banks have pleaded actual injury in the form of costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage. These injuries are not speculative and are not threatened future injuries, but are actual, current, monetary damages.").

Equifax serves in such a system."[46] The Plaintiffs allege that their "current and/or future customers have had their PII compromised, thereby undermining the integrity of the credit reporting system, which has harmed and will continue to harm [the Plaintiffs]."[47] As a result, the Plaintiffs allege the following injuries:

> FI Plaintiffs and the Class also have incurred, and will continue to incur, direct out-of-pocket costs related to investigating the impact of the Equifax Data Breach, increased monitoring for potentially fraudulent banking activity, and communicating with customers regarding their concerns about identity theft and the safety of their financial accounts in light of the Equifax Data Breach. Finally, a certainly impending risk of future harm, in the form of future fraudulent banking activity, exists as a direct result of the Equifax Data Breach. This risk of harm will continue into the foreseeable future and will require FI Plaintiffs and the Class to incur significant costs and expenses in order to reduce and mitigate this risk of harm.[48]

Other than the Financial Institution Card Issuers, the Plaintiffs do not allege that any of their information was stolen from them in the Data Breach. The injury that they claim is an injury to the "credit reporting system." This is not an injury that is concrete and particularized to the Plaintiffs. Any person or business that relies upon the provision of credit – that is, virtually everybody – can claim this injury. This theory of liability would allow every financial

---

[46] Financial Institution Pls.' Consolidated Class Action Compl. ¶¶ 12-57.

[47] *Id.*

[48] Financial Institution Pls.' Consolidated Class Action Compl. ¶ 10.

institution in the United States – and everyone else – to sue every time that there is a data breach where personally identifying information is stolen.

In fact, the Plaintiffs' own argument demonstrates how generalized their alleged injuries are. In their response brief, the Plaintiffs assert that "[e]very time a Plaintiff needs to verify the identity of a customer, because the underlying information has been compromised due to Equifax's actions, the Data Breach injures them anew."[49] Thus, according to the Plaintiffs, every time they need to rely on personally identifying information to verify a customer's identity or make a loan decision, they suffer a new injury from Equifax. This infinitely wide web of potential injuries is neither concrete nor particularized.

The alleged injury is not actual or imminent. The Consolidated Amended Complaint was filed approximately nine months after the Data Breach was disclosed. The Plaintiffs do not identify a single actual instance of identity theft of one of their customers that can be traced to the Equifax Data Breach. The Plaintiffs do not identify a single fraudulent account that has been opened using data from the Data Breach. The harm that they say that they seek to avoid is entirely conjectural and hypothetical. And, according to the Plaintiffs, the risk of this type of fraud continues forever once a Social Security number has been stolen. Some of the other injuries that the Plaintiffs allege – such as consumers abandoning credit applications if they do not get instant retail credit, lost fees

---

[49] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 13.

and interest to financial institutions due to credit freezes – are even more speculative and hypothetical.[50] It is not enough to allege facts from which it is possible to "imagine" an injury.[51] In this context, the actions that the Plaintiffs have taken, such as increased monitoring for fraudulent activity and communicating with customers, are no more than due diligence and business as usual in the digital age. The Plaintiffs cannot manufacture standing by going beyond what is required by ordinary due diligence and regulatory compliance.

None of the Financial Institutions except the Card Issuers allege that they have actually experienced fraudulent accounts or other fraudulent activity. Instead, these Plaintiffs assert that their customers' personally identifying information has been compromised, and as a result, they face an increased risk of future fraudulent activity, and cannot rely upon the credit reporting system in general. In most of the cases relied upon by the Plaintiffs where the court found that a substantial risk existed, some of the plaintiffs had alleged that fraudulent activity had already occurred.[52] These allegations of actual fraud

---

[50] *Id.* ¶¶ 256-260.

[51] *Bochese v. Town of Ponce Inlet*, 405 F.3d 964, 976 (11th Cir. 2005); *Aaron Private Clinic Management LLC v. Berry*, No. 17-15144, 2019 WL 101166, at *4 (11th Cir. Jan. 4, 2019).

[52] *See, e.g.*, *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) ("Indeed, the plaintiffs who alleged that the hackers had already commandeered their accounts or identities using information taken from Zappos specifically alleged that they suffered financial losses because of the Zappos data breach (which is why the district court held that they had standing). Although those plaintiffs' claims are not at issue in this appeal, their alleged harm undermines

strengthened the argument that a substantial risk of future harm existed. In contrast, none of the Plaintiffs here allege that fraudulent accounts have already been opened. Instead, they mostly rely upon an injury to the "general" ecosystem of the credit reporting system. This conclusion is further bolstered by the fact that the Plaintiffs have largely asserted generic allegations concerning these injuries. Although the Plaintiffs may have been harmed in similar ways by the Data Breach, as they insist,[53] they still must show a concrete, personal injury-in-fact. The strength of the Plaintiffs' allegations concerning a substantial risk of future fraudulent activity, and the steps they have taken in response to that risk, are discounted by the fact that the Plaintiffs all assert the same, generic allegations about a substantial risk of future harm.

The Plaintiffs also argue that they did not manufacture an injury because federal law required them to investigate the Data Breach and take action to protect their customers.[54] According to the Plaintiffs, they did not voluntarily take action in response to the Data Breach, but instead had no choice under federal law but to incur costs in response to the Data Breach to remain in compliance. However, the Plaintiffs rely upon general regulatory obligations that require them to develop security programs and identify risks to their

---

Zappos's assertion that the data stolen in the breach cannot be used for fraud or identity theft.").

[53] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 11 n.15.

[54] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 13-15.

customer information. For instance, regulations implementing the Gramm-Leach-Bliley Act provide that financial institutions must, among other things, "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."[55] Furthermore, rules promulgated under the FCRA require the Plaintiffs to develop and implement programs that are "designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account."[56] These general obligations to study risks to data security and mitigate identity theft are insufficient to confer standing. Concluding otherwise would mean that financial institutions have standing to assert a claim any time some event occurs that affects the data security landscape. This would be unworkable.

And, the cases that the Plaintiffs cite in support of this proposition are distinguishable. For example, in *Wells v. Willow Lake Estates, Inc.*, the plaintiffs alleged that the defendant, a mobile home community, selectively enforced its regulations regarding home and lawn appearance against the

---

[55] 16 C.F.R. § 314.4(b).

[56] 16 C.F.R. § 681.1(d)(1).

plaintiffs because they were disabled and because of their nationality.[57] The court found that the plaintiffs adequately pleaded an injury because they alleged that "they have already been forced to spend time and money complying with regulations that Willow Lakes has selectively enforced against them."[58] This conclusion, that the costs incurred to comply with the pretextual, discriminatory enforcement of a housing community rule can constitute an injury, is far from providing a general rule that additional costs incurred to comply with any regulatory obligation can confer standing. The costs that the *Wells* plaintiffs incurred to comply with the defendant's discriminatory enforcement of its own regulations represent a much more concrete and particularized injury than the costs incurred by the Plaintiffs to comply with general regulations about data security.[59] Such a formulation would allow any plaintiff to have standing against any defendant whose conduct may have had a slight, peripheral effect on that

---

[57] *Wells v. Willow Lake Estates, Inc.*, 390 F. App'x 956, 957 (11th Cir. 2010).

[58] *Id.* at 959.

[59] The other case the Plaintiffs rely upon is similarly distinguishable. *See* Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 15. In *City of Waukesha v. E.P.A.*, the plaintiffs challenged EPA regulations establishing standards for radionuclide levels in public water systems. *See City of Waukesha v. E.P.A.*, 320 F.3d 228, 231 (D.C. Cir. 2003). The court concluded that the City of Waukesha had standing because it would face substantial costs in complying with the challenged regulations. *See id.* at 234. This conclusion, that a city has standing to challenge a regulation that it would incur costs to comply with, is very different from the Plaintiffs' argument that they have been injured *by Equifax* due to incurring costs to comply with general data security regulations *that they are not challenging*.

plaintiff's compliance costs. The Court declines to adopt such a standard. Such an injury is not concrete or particularized. Thus, the Court concludes that this argument fails to establish standing.

Next, the Defendants contend that the Plaintiffs have not adequately alleged traceability.[60] To establish standing, the Plaintiffs must allege "a causal connection between the injury and the conduct complained of—the injury has to be 'fairly ... trace[able] to the challenged action of the defendant, and not ... th[e] result [of] the independent action of some third party not before the court.'"[61] The Defendants contend that the Plaintiffs' alleged injuries are too attenuated to establish traceability. As the Plaintiffs in fact allege, the creation of "synthetic identities" using a stolen Social Security number requires a fraudster to apply for credit, creation of a credit profile by a credit reporting agency, maintaining good credit over time to build up credit limits, applying for more credit or credit cards, and then not paying when the credit limits are maxed out.[62] Thus, actual harm to a financial institution is contingent upon a lengthy sequence of actions that are far removed from the Data Breach.

The Eleventh Circuit case that the Defendants rely upon, *Florida Association of Medical Equipment Dealers, Med-Health Care v. Apfel*, is on

---

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

61 *Lujan*, 504 U.S. at 560 (quoting *Simon v. Eastern Ky. Welfare Rights Organization*, 426 U.S. 26, 41-42 (1976)).

62 Financial Institution Pls.' Consolidated Class Action Compl. ¶ 239.

point. In *Apfel*, medical equipment suppliers challenged a medical-supply bidding process on the ground that it failed to comply with a federal statute designed to ensure public access in the process.[63] The Eleventh Circuit concluded that these allegations were "much too attenuated" to confer standing.[64] The court explained that "FAMED's argument seems to be that: if FAMED were to bid, FAMED could be forced to participate in a 'tainted' bidding project, which might prove unsuccessful, and potentially threaten the livelihood of FAMED's membership should their bids be rejected."[65] Similarly, the Plaintiffs' risk of fraudulent banking activity depends upon an attenuated causal chain. Therefore, the Plaintiffs have not adequately alleged traceability. Finally, it is hard to imagine a ruling by this Court that will likely remedy "pollut[ion] of the entire financial services ecosystem."[66] Except for the payment card related claims of the Financial Institution Card Issuers, the Financial Institution Plaintiffs lack standing.

The Defendants also argue that the Financial Institution Card Issuers have failed to sufficiently allege an injury that confers standing. According to the Defendants, these Plaintiffs have only made the "generic allegation" that

---

[63] *Florida Association of Medical Equipment Dealers, Med-Health Care v. Apfel,* 194 F.3d 1227, 1229 (11th Cir. 1999).

[64] *Id.* at 1230.

[65] *Id.*

[66] Financial Institution Pls.' Consolidated Class Action Compl. ¶ 9.

they issued payment cards that were compromised by the Data Breach.[67] They argue that the Financial Institution Card Issuers have not alleged that these affected payment cards have suffered fraudulent charges.[68] However, the Court concludes that the Financial Institution Card Issuers have adequately alleged an injury resulting from compromised payment card data. In the Complaint, the Financial Institution Card Issuers allege that payment cards that they issued were compromised in the Data Breach, and that they received fraud alerts relating to these compromised cards. Even if some of the Financial Institution Card Issuers did not allege that any of these comprised payment cards had already experienced unauthorized charges as a result of the Data Breach, they have still alleged that they incurred costs of reissuing these cards to customers. These costs associated with replacing their payment cards constitute sufficient injury to confer standing. Even if these allegations may be generic to a degree, the injuries associated with reissuing payment cards are concrete and easily ascertainable. Therefore, the Court finds these allegations sufficient to establish standing as to these Plaintiffs.

2. The Associations

Finally, the Defendants contend that the Association Plaintiffs lack

---

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

68 *Id.*

standing.[69] To establish standing, an association plaintiff must show: "(1) its members otherwise have standing to sue in their own right; (2) the interests the plaintiff-association seeks to protect are germane to the association's purpose; and (3) neither the claim asserted nor the relief requested must require the participation of the association's members."[70] An association can also establish standing under the "diversion-of-resources theory" by showing that the defendant's acts forced the organization to divert its resources to respond to these acts.[71] The Defendants contend that the Association Plaintiffs have failed to establish these requirements.

First, the Defendants contend that these Plaintiffs have failed to show that their members have standing to sue. According to the Defendants, the Association Plaintiffs have not identified their specific members who have standing. This requirement to identify a member is not required when all the members of an organization are affected by the conduct.[72] For the reasons set forth above, only the Financial Institution Card Issuers have standing. From the Consolidated Amended Complaint, it is impossible to tell whether any members of the Association Plaintiffs have standing. If, as the Defendants contend, the

---

[69] Defs.' Mot. to Dismiss, at 25-27.

[70] *Greater Atlanta Home Builders Ass'n, Inc. v. City of Atlanta, Ga.*, 149 F. App'x 846, 848 (11th Cir. 2015).

[71] *See Havens Realty Corp. v. Coleman*, 455 U.S. 363, 379 (1982).

[72] *See Summers v. Earth Island Inst.*, 555 U.S. 488, 499 (2009).

vast majority of the compromised credit cards were issued by a few huge banks, none of the Associations' members may have standing. Failure to identify an injured constituent prevents an association from asserting associational standing.[73]

The Association Plaintiffs have also failed to establish standing under a diversion-of-resources theory. The Supreme Court has held that a "concrete and demonstrable injury to the organization's activities—with the consequent drain on the organization's resources—constitutes far more than simply a setback to the organization's abstract social interests" and is sufficient to establish standing.[74] The Association Plaintiffs fail to allege facts showing a concrete and particularized injury. The only allegations of injury are generic and abstract. The Motion to Dismiss should be granted as to the Association Plaintiffs for lack of standing.

C. Negligence

The remainder of this Opinion and Order applies only to the surviving claims of the Financial Institution Card Issuers. The Defendants move to dismiss the Plaintiffs' negligence claim.[75] In Count 1 of the Consolidated Amended Complaint, the Plaintiffs allege that Equifax owed a duty to the

---

[73] *Nat'l All. for Mentally Ill, St. Johns Inc. v. Bd. of Cty. Comm'rs of St. Johns Cty.*, 376 F.3d 1292, 1296 (11th Cir. 2004).

[74] *Havens Realty Corp.*, 455 U.S. at 379.

[75] Defs.' Mot. to Dismiss, at 24.

Plaintiffs to "use reasonable care to avoid causing foreseeable risk of harm to FI Plaintiffs and members of the Class when obtaining, storing, using, selling, and managing PII and Payment Card Data, including taking action to reasonably safeguard such data and providing notification to FI Plaintiffs and the Class of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses."[76] The Plaintiffs also allege that Equifax had a duty of care that arose from GLBA and the FCRA.[77] The Defendants contend that they were under no duty of care toward the Plaintiffs.

1. Duty

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."[78] "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."[79] Whether such a duty exists is a question of

---

[76] Financial Institution Pls.' Consolidated Class Action Compl. ¶ 281.

[77] *Id.* ¶¶ 287, 298.

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

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

law.[80] Georgia recognizes a general duty "to all the world not to subject them to an unreasonable risk of harm."[81] "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[.]"[82] Failure to exercise ordinary care with respect to payment card numbers creates a foreseeable risk of injury to the card issuers.[67]

The Defendants argue that Georgia law does not impose a duty of care to safeguard personal information.[68] The Defendants rely primarily upon a recent Georgia Court of Appeals case, *McConnell v. Georgia Department of Labor*.[69] 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.[70] This email included a spreadsheet with the name, Social Security number, phone number, email address, and age of 4,000

---

80 *Id.* (internal quotations omitted).

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

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

67 *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).

68 Defs.' Mot. to Dismiss, at 28.

69 *Id.*

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

Georgians who had registered for services with the agency.[71] The plaintiff, whose information was disclosed, filed a class action, asserting, among other claims, a claim for negligence.[72]

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.[73] 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.[74] The court concluded that neither of these statutory sources gave rise to a duty to safeguard personal information.[75] 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."[76] However, in doing so, the court 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

---

71 *Id.*

72 *Id.*

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

74 *Id.* at 460.

75 *Id.* at 461-62.

76 *Id.* at 462.

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."[77]

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.[78] On remand, the Georgia Court of Appeals, after deciding that sovereign immunity did not bar the plaintiff's claims, once again concluded that 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."[79] 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.[80] Although the legislature showed a "concern about the cost of identity theft to the

---

[77] *Id.* at 460 n.4.

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

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

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

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."[81]

The Defendants contend that *McConnell III* confirms that there is no duty under Georgia law, common law or statutory, to safeguard personally identifiable information.[82] 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 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.[83] The failure to maintain reasonable and appropriate data security for consumers' sensitive

---

81 *Id.* at 679.

82 Defs.' Mot. to Dismiss, at 28-31.

83 *See* 15 U. S. C. § 1681b(a).

personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.[84] The Gramm–Leach–Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information.[85] The FTC has done that.[86]

The Plaintiffs, in turn, 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.[87] The Plaintiffs rely primarily upon *Home Depot* and *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.[88] 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."[89] 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

---

[84] 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).

[85] *See* 15 U.S.C. § 6801(b).

[86] *See* 16 C.F.R. §314.4(b-e).

[87] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 25-34.

[88] *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).

[89] *Id.* at *3.

not to subject them to an unreasonable risk of harm."[90] 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."[91]

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 existence of a plausible legal duty and survive a motion to dismiss."[92] 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.[93] 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

---

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

[91] *Id.* at *4.

[92] *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).

[93] *Id.* at *5.

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.*[94] 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.[95]

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 personal information.[96] Thus, according to the Defendants, *Home Depot* and *Arby's* are no longer good law.[97] 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.[98] 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

---

94 *Id.* at *6.

95 *Id.* at *7.

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

97 *Id.*

98 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 26-27.

foreseeable.[99] 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.[100]

The Court concludes that, under the facts alleged in the Complaint, the Defendants owed the Plaintiffs a duty of care to safeguard the Financial Institution Card Issuers' information in its custody. This duty of care arises from the allegations that the Defendants knew of a foreseeable risk to the data security systems of Equifax but failed to implement reasonable security measures. *McConnell III* does not alter this conclusion. As 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.[101] Such allegations did not exist in the *McConnell* line of cases.[102] 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

---

99 *Id.* at 14-15.

100 *Id.* at 16.

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

102 *Id.*

distinction. Thus, this Court reads *McConnell III* as holding that, in the absence of a foreseeable risk, no general duty to safeguard personal information exists under Georgia common law, the Georgia Personal Identity Protection Act, or the Georgia Fair Business Practices Act. 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.[103]

The Defendants then argue that the Plaintiffs' negligence claim fails because "mere foreseeability" is not a basis, on its own, for imposing a duty of care.[104] Instead, according to the Defendants, foreseeability is just one factor to consider when evaluating the existence of a legal duty.[105] While it is true that the mere foreseeability of harm is not sufficient on its own to establish a duty of care, the Plaintiffs' negligence claims rest on more than just foreseeability. The Plaintiffs allege that the Defendants subjected them to an unreasonable risk of foreseeable harm by collecting troves of valuable personal data and failing to take reasonable security measures in the face of known risks. By subjecting the Plaintiffs to this unreasonable risk of harm, the Defendants were under a duty to take reasonable measures to protect this data from foreseeable

---

[103] *See Home Depot*, 2016 WL 2897520, at *4.

[104] Defs.' Reply Br., at 11-12.

[105] *Id.* at 12.

harms. The Defendants collected valuable information relating to the Financial Institution Card Issuers' payment cards, knew that this information was valuable, and knew that serious security risks existed. Yet, according to the Complaint, they failed to take reasonable actions to protect this valuable information in their custody. The Court concludes that these allegations adequately establish a claim for negligence under Georgia law.

The Plaintiffs also argue that Equifax voluntarily assumed a duty to handle their payment card data with reasonable care.[106] Under Georgia law, "one who undertakes to do an act or perform a service for another has the duty to exercise care, and is liable for injury resulting from his failure to do so, even though his undertaking is purely voluntary or even though it was completely gratuitous, and he was not under any obligation to do such act or perform such service, or there was no consideration for the promise or undertaking sufficient to support an action ex contractu based thereon."[107] "Where one undertakes an act which he has no duty to perform and another reasonably relies upon that undertaking, the act must generally be performed with ordinary or reasonable care."[108] According to the Plaintiffs, the Defendants voluntarily decided to collect the Defendants' personal information and payment card data, and voluntarily

---

106 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 34-35.

107 *Stelts v. Epperson*, 201 Ga. App. 405, 406 (1991).

108 *Id.*

assumed "a duty to comply with applicable federal and state laws and protect the PII it collected."[109] However, the Defendants did not voluntarily undertake to perform a service for the Plaintiffs. Instead, the Defendants collected this data as a part of their own business operations. This "Good Samaritan" principle of liability does not apply, because Equifax did not negligently perform a voluntary duty it assumed with regard to the Plaintiffs.[110] Thus, the Defendants did not voluntarily assume a legal duty of care toward the Plaintiffs.[111]

2. Causation

Next, the Defendants assert that the Plaintiffs have failed to establish causation. Specifically, the Defendants assert that the Plaintiffs' harms were caused by their customers' concerns, and not by the Defendants.[112] However, this argument does not apply to the payment card claims asserted by the Financial Institution Card Issuers. "[B]efore any negligence, even if proven, can be

---

[109] Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 34.

[110] *See Cmty. Fed. Sav. & Loan Ass'n v. Foster Developers, Inc.*, 179 Ga. App. 861, 865 (1986) ("Thus, having taken the aegis of a 'Good Samaritan,' one is responsible for negligently performing the duties assumed.").

[111] The Defendants also contend that they did not breach a legal duty of care toward the Plaintiffs by failing to disclose the Data Breach. *See* Defs.' Mot. to Dismiss, at 34-35. In the Complaint, the Plaintiffs allege that the Defendants owed them a common law duty to, among other things, "provid[e] notification . . . of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses." Financial Institution Pls.' Consolidated Am. Compl. ¶ 281. The Plaintiffs fail to respond to this argument. Therefore, to the extent that the Plaintiffs assert a negligence claim premised upon a legal duty to notify them of the Data Breach, that claim is deemed abandoned.

[112] Defs.' Mot. to Dismiss, at 35-36.

actionable, that negligence must be the proximate cause of the injuries sued upon."[113] "To establish proximate cause, a plaintiff must show a legally attributable causal connection between the defendant's conduct and the alleged injury."[114] The key question with regard to causation analysis is foreseeability.[115] As discussed above, it was reasonably foreseeable to the Defendants that financial institutions such as the card issuer Plaintiffs would need to incur costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage, in the event of a breach of Equifax's systems. Therefore, under Georgia law, the Plaintiffs have adequately pleaded causation.

3. Damages

Next, the Defendants contend that the Plaintiffs have failed to adequately plead a legally cognizable injury.[116] "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."[117] The Defendants rely upon a recent Georgia Court of Appeals case,

---

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

114 *Id.*

115 *Byrd v. English*, 117 Ga. 191 (1903).

116 Defs.' Mot. to Dismiss, at 39-41.

117 *Whitehead v. Cuffie*, 185 Ga. App. 351, 353 (1987).

Collins v. Athens Orthopedic Clinic. There, the defendant's patients sued after a cyberhacker stole their personal information from the defendant's systems.[118] The court concluded that the plaintiffs did not allege a legally cognizable harm.[119] 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.[120]

Thus, according to the Defendants, the Plaintiffs' claims must fail, since costs associated with protecting the plaintiffs' *own* personal information in *Collins* failed to establish a sufficient injury.[121]

However, *Collins* is distinguishable. There, the plaintiffs alleged only an "increased risk of harm" associated with taking precautionary measures.[122] 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 Financial Institution Card Issuers here have not pleaded merely an increased risk of

---

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

119 *Id.* at 18.

120 *Id.*

121 Defs.' Mot. to Dismiss, at 41.

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

harm. Instead, they have alleged that they have already incurred significant costs in response to the Data Breach. The Court concludes that these allegations are sufficient.

Finally, the Defendants argue that the economic loss rule precludes the Plaintiffs' negligence claim. According to the Defendants, the Plaintiffs merely allege economic losses, and not harm to person or property, resulting from the Data Breach.[123] "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."[124] In other words, "a plaintiff may not recover in tort for purely economic damages arising from a breach of contract."[125] Where, 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."[126] 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

---

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

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

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

[126] *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).

data on their networks have a duty to protect that information[.]"[127] As discussed above, the Defendants owed the Plaintiffs a duty of care to take reasonable measures to safeguard their payment card data. Therefore, since an independent duty existed, the economic loss rule does not apply.

D. Negligence Per Se

Next, the Defendants move to dismiss the Plaintiffs' negligence per se claim.[128] In Count 2 of the Complaint, the Plaintiffs allege that Equifax violated the Gramm-Leach-Bliley Act, Section 5 of the FTC Act, and similar state statutes, by maintaining security programs and safeguards that "were not appropriate to Equifax's size and complexity" and by "mishandling consumer data and not using reasonable measures to protect PII and by not complying with applicable industry standards."[129] "Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se."[130] 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

---

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

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

129 Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 313, 318-19.

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

suffered.[131]

1. GLBA

The Defendants first argue that the Gramm-Leach-Bliley Act (the "GLBA") and its implementing regulations cannot provide a basis for a negligence per se claim.[132] The GLBA provides, in part, that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[133] In *Wells Fargo Bank, N.A. v. Jenkins*, the Georgia Supreme Court concluded that the GLBA could not form the basis of a negligence claim.[134] The court noted that the GLBA "certainly . . . expresses the goal that financial institutions respect the privacy, security, and confidentiality of customers."[135] However, it explained that "[w]hile this is a clear Congressional policy statement, it is just that. It does not provide for certain duties or the performance of or refraining from any specific acts on the part of financial institutions, nor does it articulate or imply a

---

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

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

133 15 U.S.C. § 6801(a).

134 *See Wells Fargo Bank, N.A. v. Jenkins*, 293 Ga. 162, 164-65 (2013).

135 *Id.* at 164.

standard of conduct or care, ordinary or otherwise."[136] "Congress did not see fit to impose such a duty under 15 U.S.C. § 6801(a) . . . ."[137]

This Court agrees. The GLBA does not provide a specific standard of conduct that is sufficient to give rise to a legal duty under Georgia law. The cases that the Plaintiffs rely upon do not support an argument to the contrary. In most of those cases, the issue of whether the GLBA imposes a legal duty of care was not at issue, or they contain no discussion of the standard of conduct that the GLBA actually imposes. Thus, the Court concludes that the Plaintiffs' negligence per se claims must be dismissed to the extent that they are predicated upon the GLBA.

However, the Plaintiffs also allege that the Defendants breached a statutory duty owed under the regulations implementing the GLBA.[138] The Plaintiffs argue that the failure to maintain reasonable data security measures to protect consumer information violates the Safeguards Rule, which constitutes a violation of the GLBA.[139] The Safeguards Rule, 16 C.F.R. § 314, implements the GLBA by setting forth "standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to

---

136 *Id.*

137 *Id.* at 165.

138 *See, e.g.*, Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 314-15.

139 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 43-46.

protect the security, confidentiality, and integrity of customer information."[140] The Defendants contend that the Safeguards Rule, like the GLBA itself, cannot serve as the basis for a statutory duty because it merely provides general requirements for data security, and does not provide an ascertainable standard of conduct.[141] In *Jenkins*, the Georgia Supreme Court, in rejecting a statutory duty under the GLBA, noted that "[t]here is no finding by the Court of Appeals of a violation of any regulation, directive, or standard authorized by 15 U.S.C. § 6801(b), to support Jenkins's claim of the Bank's negligence."[142] It noted that "Jenkins points to certain provisions of the Code of Federal Regulations in support of the finding of a duty under 15 U.S.C. § 6801(a), specifically 16 C.F.R. § 314.1; however, the regulation was not part of the Court of Appeals analysis or its finding of duty under the GLBA. Furthermore, 16 C.F.R. § 314.1(a) expressly implements only sections 501 and 505(b)(2) of the GLBA and applies to those financial institutions over which the Federal Trade Commission has jurisdiction."[143]

However, unlike the GLBA itself, the Court concludes that the Safeguards Rule provides an ascertainable standard of conduct permitting it to serve as the basis for a negligence per se claim. In *Jenkins*, the Georgia Supreme Court

---

140 16 C.F.R. § 314.1(a).

141 Defs.' Mot. to Dismiss, at 44-46.

142 *Wells Fargo Bank, N.A. v. Jenkins*, 293 Ga. 162, 165 (2013).

143 *Id.* at 165 n.3.

rejected such a claim under the GLBA because it did "not provide for certain duties or the performance of or refraining from any specific acts on the part of financial institutions, nor does it articulate or imply a standard of conduct or care, ordinary or otherwise."[144] In contrast to the GLBA, the Safeguards Rule provides for certain duties that financial institutions must perform, and provides an ascertainable standard of conduct. For example, it provides that financial institutions should "[d]esignate an employee or employees to coordinate your information security program."[145] It further requires these institutions to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks."[146] It explains that such a risk assessment should include consideration of "[e]mployee training and management," "[i]nformation systems, including network and software design, as well as information processing, storage, transmission and disposal," and "[d]etecting, preventing and responding to attacks, intrusions, or other systems failures."[147] The Court finds that these provisions go beyond a mere policy statement and provide a specific

---

144 *Id.* at 164.

145 16 C.F.R. § 314.4(a).

146 16 C.F.R. § 314.4(b).

147 16 C.F.R. § 314.4(b)(1)-(3).

standard of conduct.[148]

The Defendants then contend that the Plaintiffs do not provide any allegations that the Defendants breached this standard of conduct.[149] However, the Court concludes that the Plaintiffs' allegations are sufficient. The Plaintiffs allege that the Defendants breached their duty under the Safeguards Rule because their data security systems "were not adequate to: identify reasonably foreseeable internal and external risks, assess the sufficiency of safeguards in place to control for these risks, or to detect, prevent, or respond to a data breach."[150] They further allege that "Equifax's security program and safeguards were inadequate to evaluate and adjust to events that would have a material impact on Equifax's information security program, such as the numerous prior data breaches that other retailers and Equifax itself had experienced and the notification to Equifax that an identified vulnerability in a software program it utilized would make Equifax particularly susceptible to a data breach."[151] These

---

148 The Court acknowledges that the cases cited by the Plaintiffs do not support this conclusion. In those cases, whether the regulations could serve as the basis for a statutory duty were not at issue. *See, e.g.*, *Owens v. Dixie Motor Co.*, No. 5:12-CV-389-FL, 2014 WL 12703392, at *14 (E.D.N.C. Mar. 31, 2014) (concluding that a showing of severe emotional distress is not necessary for a negligence per se claim). However, the Defendants also do not point to any cases to the contrary. Based upon a reading of the regulations at issue, and Georgia caselaw pertaining to negligence per se, the Court concludes that these regulations under the GLBA can provide a statutory duty.

149 Defs.' Mot. to Dismiss, at 46.

150 Financial Institution Pls.' Consolidated Am. Compl. ¶ 313.

151 *Id.*

allegations are sufficient to avoid dismissal.

2. FTC Act

The Defendants then argue that the FTC Act fails to impose a duty with specificity upon the Defendants. Here, the Plaintiffs allege that the Defendants violated Section 5 of the FTC Act. The Defendants argue that Section 5 cannot form the basis of a negligence per se claim. The Complaint 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. 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.[152] The Defendants' Motion to Dismiss the negligence per se claim should be denied.

The Defendants, acknowledging that this Court has allowed negligence per se claims under Section 5 of the FTC Act to proceed in *Arby's* and *Home Depot*, argue that this case's distinct factual circumstances, and the Eleventh Circuit's recent ruling in *LabMD, Inc. v. Federal Trade Commission*, justify departing from the reasoning of those prior cases.[153] This case, like those prior cases, asks whether Section 5 imposes a legal duty to safeguard personally

---

[152] *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).

[153] Defs.' Mot. to Dismiss, at 36 n.10.

identifiable information in a business's custody.

Second, the Defendants argue that *LabMD* should lead this Court to a different conclusion. However, that was a direct enforcement action in which the court 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. There, the Eleventh Circuit noted that "standards of unfairness" must be found "in 'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law."[154] 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." However, the Defendants misread *LabMD*. There, the court merely stated that the FTC, in issuing standards of fairness, must provide the sources of such standards it enforces, and assumed in that case that the common law was the source.[155] Instead, plaintiffs can rely upon Section 5 as it has been defined by the FTC, and rely upon those definitions.[156] Thus, the Court finds this argument unpersuasive.

The Defendants also argue that this claim fails because there is no

---

[154] *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221, 1231 (11th Cir. 2018).

[155] *Id.*

[156] *Id.* at 1232.

private cause of action under the FTC Act.[157] However, the Court finds this argument unpersuasive. The Defendants conflate private rights of action with negligence per se. Under Georgia law, a statute can serve as the basis of a negligence per se claim even if it does itself provide a private right of action.[158] These statues "merely provide the source of duty that is owed, but do not govern the right of action available or the course of the proceedings."[159] Therefore, Section 5 of the FTC Act can provide a statutory duty for a negligence per se claim, even if the underlying statute does not itself provide a private right of action.

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."[160] Even if negligence per se is shown, a plaintiff must still prove proximate causation and actual damage to recover.[161] As discussed above, the Court concludes that the Plaintiffs have sufficiently alleged both a legally cognizable injury and proximate causation. Therefore, this argument is

---

157 Defs.' Mot. to Dismiss, at 47-48.

158 *Pulte Home v. Simerly*, 322 Ga. App. 699, 706-07 (2013) ("Pulte has not cited authority, nor can we find any, that a plaintiff, who pursues a negligence per se action based on violations of the CWA or state statutes implementing the CWA, is subject to the CWA's requirements regarding private citizen lawsuits.").

159 *Id.* at 706.

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

161 *Id.*

unavailing.

E. Negligent Misrepresentation

Next, the Defendants contend that the Plaintiffs fail to sufficiently plead a claim for negligent misrepresentation.[162] The essential elements of a negligent misrepresentation claim under Georgia law are "(1) the defendant's negligent supply of false information to foreseeable persons, known or unknown; (2) such persons' reasonable reliance upon that false information; and (3) economic injury proximately resulting from such reliance."[163]

The Defendants first contend that the Plaintiffs fail to plead their negligent misrepresentation claim with the requisite specificity.[164] However, the heightened pleading standards of Rule 9(b) do not apply to claims of negligent misrepresentation.[165] But, even if Rule 9(b) were to apply, the Plaintiffs' allegations would likely suffice. The Plaintiffs have alleged the specific misrepresentations that the Defendants made, which Defendants made them, how such representations were false, and why the Defendants knew or should

---

[162] Defs.' Mot. to Dismiss, at 49.

[163] *Hardaway Co. v. Parsons, Brinckerhoff, Quade & Douglas, Inc.*, 267 Ga. 424, 426 (1997).

[164] Defs.' Mot. to Dismiss, at 49.

[165] *See Higgins v. Bank of America, N.A.*, 115CV01119ELRJFK, 2015 WL 12086083, at *4 (N.D. Ga. Sept. 22, 2015) ("[T]he particularity requirements for pleading fraud are not applicable to Plaintiff's negligent misrepresentation claim.").

have known that those statements were false.[166] Such allegations are sufficient. Furthermore, the Plaintiffs also allege that the Defendants knew the Plaintiffs would rely upon such representations, due to the importance of maintaining such cybersecurity.[167] These allegations are sufficient to state a claim for negligent misrepresentation under Georgia law.

The Defendants also argue the Plaintiffs have failed to allege that the purported misrepresentations caused them any injury.[168] To successfully plead a claim for negligent misrepresentation under Georgia law, a plaintiff must allege that economic injury proximately resulted from reliance upon the defendant's misrepresentations.[169] The Plaintiffs' allegations satisfy this requirement. In the Complaint, the Plaintiffs allege that financial institutions would not provide sensitive data to Equifax if they did not believe that it maintained strict data security standards.[170] The Plaintiffs further allege that they relied upon the Defendants' misrepresentations as to the manner in which Equifax stored this data, and that due to this reliance, they suffered injuries as

---

166 *See, e.g.*, Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 151-64.

167 *Id.* ¶¶ 126, 134-36.

168 Defs.' Mot. to Dismiss, at 51.

169 *Greenwald v. Odom*, 314 Ga. App. 46, 52 (2012).

170 Financial Institution Pls.' Consolidated Am. Compl. ¶ 333.

a result of the compromise of the payment card data entrusted to Equifax.[171] These allegations are sufficient to establish a claim for negligent misrepresentation at this stage of the proceedings.

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 consumer transactions and consumer acts or practices in trade or commerce."[172] 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).[173] 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.[174] According to the Defendants, *McConnell III* would have been decided differently if the Georgia Fair Business Practices Act contained such a requirement.[175] In *McConnell III*, the court concluded that part of the Georgia Fair Business

---

171 *Id.* ¶¶ 134-36, 336-337.

172 O.C.G.A. § 10-1-393(a).

173 Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 339-59.

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

175 *Id.* at 38.

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."[176] That provision prohibits "intentionally communicating a person's social security number."[177] The court rejected the plaintiff's claim, noting that he had alleged that the defendant negligently disseminated his social security number.[178] The Court agrees.

The Plaintiffs make multiple arguments in response. However, the Court finds these arguments unpersuasive. First, 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.[179] 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

---

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

177 *Id.* (emphasis omitted).

178 *Id.*

179 *McConnell III*, 345 Ga. App. 669, 677-79.

protection and data breach laws.[180] Even though *McConnell III* examined the 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.

G. Foreign State Fraud and Consumer Protection Statutes

Next, the Defendants move to dismiss the Plaintiffs' claims under foreign state business fraud and consumer protection statutes. First, the Defendants contend that the deceptive trade practice laws of foreign states cannot be applied to conduct that took place in Georgia.[181] The Defendants argue that these state statutes do not extend to conduct that occurred in Georgia. In 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. 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

---

180 *Id.* at 679.

181 Defs.' Mot. to Dismiss, at 54-55.

the specific consumer protection statutes asserted by the Plaintiffs only extend to conduct taking place within the states. They do not stand for the proposition that the statutes only apply to conduct that takes place within those states. The Plaintiffs, who allege that they were harmed in each of these respective states, have adequately stated claims under these state statutes.[182]

Second, the Defendants argue that these foreign states lack authority under the Constitution to govern conduct occurring in Georgia.[183] The Defendants cite *State Farm Mutual Automobile Insurance Company v. Campbell*.[184] In *State Farm*, the Supreme Court imposed extraterritorial limitations on punitive damages awards.[185] 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."[186] *State Farm* does not stand for the proposition that, because all of

---

[182] *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.").

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

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

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

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

a defendant's conduct occurred outside of a state, that state cannot enforce its laws against that defendant.[187] Out-of-state conduct that results in injuries inside of a state "does not constitute lawful out-of-state conduct or conduct related to other persons."[188] 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.[189] However, even assuming this is true, the Plaintiffs have alleged that these acts that occurred in Georgia resulted in injuries in other states. These out-of-state injuries fall within the ambit of many of these foreign state statutes.[190] Therefore, this argument is unavailing.

The Defendants also cite *Healy v. Beer Institute, Inc.*[191] There, the Supreme Court concluded that, under the Dormant Commerce Clause, "a statute that directly controls commerce occurring wholly outside the boundaries of a

---

187 *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.").

188 *Id.*

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

190 *See Hendricks v. Ford Motor Co.*, 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.").

191 *Healy v. Beer Inst., Inc.*, 491 U.S. 324 (1989).

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."[192] 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."[193] 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."[194] 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 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.[195] However, as explained above, Equifax can be held liable, despite the intervening act of the criminal hackers, due to their 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

---

192 *Id.* at 336.

193 *Id.* (internal quotations omitted).

194 *Id.* at 339 (internal quotations omitted).

195 Defs.' Mot. to Dismiss, at 56.

third parties. Therefore, this argument is unpersuasive.

Second, the Defendants contend that the Plaintiffs have not adequately pleaded claims under these state statutes.[196] The Defendants contend that the Plaintiffs have failed to adequately plead fraud.[197] However, as the Plaintiffs correctly point out, many of the statutes under which they assert claims do not require the elements of fraud. "[C]onsumer protection claims are not claims of fraud, even if there is a deceptive dimension to them."[198] First, with regard to the Plaintiffs' state law claims for "unfair practices," the Defendants have failed to demonstrate that such claims contain the elements of fraud as essential elements.[199] Instead, most of these statutes require a showing that a defendant acted "unfairly," "immorally," with "reprehensible conduct," and so on.[200] The Defendants do not explain how the Plaintiffs fail to meet the elements of these statutes.

The Plaintiffs also argue that their claims for "deceptive acts" under these statutes also do not require a showing of the elements of fraud.[201] The Court

---

196 Defs.' Mot. to Dismiss, at 57.

197 *Id.*

198 *Consumer Fin. Protection Bureau v. RD Legal Funding, LLC*, 332 F. Supp. 3d 729, 768 (S.D.N.Y. 2018) (internal quotations omitted).

199 *See* [Doc. 471-1].

200 *Id.*

201 Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, at 57.

agrees that the Plaintiffs are not required to plead fraud with particularity with regard to the state statutes.[202] Rule 9(b) requires a complaint to "state with particularity the circumstances constituting fraud."[203] "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 gained as a consequence of the fraud."[204] 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.[205]

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."[206] "A claim 'sounds in fraud' when a plaintiff alleges 'a unified course of fraudulent conduct and rel[ies] entirely on that course of

---

[202] *Id.* at 56-59.

[203] FED. R. CIV. P. 9(b).

[204] *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)).

[205] Defs.' Mot. to Dismiss, at 57.

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

conduct as the basis of [that] claim.'"[207] 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.[208] The court noted that, "to sound in fraud," it is not enough that a claim be "near enough to fraud, or fraud-like" for Rule 9(b) to apply.[209] 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.[210]

Here, the Defendants have failed to show that 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.

Next, the Defendants contend that the Plaintiffs have not adequately pleaded scienter and injury.[211] With regard to scienter, the Defendants contend

---

[207] *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).

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

[209] *Id.* at 1287.

[210] *Id.*

[211] Defs.' Mot. to Dismiss, at 58-59.

that the Plaintiffs have only alleged conclusory legal conclusions.[212] First, the Defendants have failed to explain which claims the Plaintiffs fail to adequately allege scienter. Second, even assuming scienter is a necessary element of these state statutes, the Plaintiffs have made sufficient allegations. In the Complaint, the Plaintiffs allege that Equifax knew that its data security measures were insufficient, that it knew of widely-publicized data breaches at similar companies, that it knew that it had deprioritized cybersecurity, and that it knew that the data in its custody was a valuable target.[213] These allegations adequately establish scienter.

Next, the Defendants argue that the Plaintiffs have not adequately alleged injury under these state statutes.[214] However, as discussed above with regard to both standing and negligence, the Plaintiffs have alleged legally cognizable harms. The Defendants also contend that the Plaintiffs must assert injuries that are "ascertainable" and "monetary."[215] The Defendants cite one case for this proposition. However, the Court concludes that the Financial Institution Card Issuers have alleged injuries that are ascertainable and monetary. These Plaintiffs assert that they incurred costs in responding to the compromise of

---

212 *Id.*

213 *See* Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 124-36, 137-49, 150-61.

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

215 *Id.*

their payment card data, including cancelling and reissuing these payment cards. These alleged injuries are monetary and easily ascertainable.

Then, the Defendants argue that the Plaintiffs assert claims under statutes that only provide equitable relief.[216] According to the Defendants, the Plaintiffs seek monetary damages under Minnesota and Nebraska statutes that only provide for equitable relief.[217] The Plaintiffs concede that they are not seeking monetary damages under these statutes, but instead are requesting all monetary and non-monetary relief allowed by law, including attorneys' fees.[218] Therefore, the Court concludes that the Plaintiffs cannot seek monetary damages under these statutes.

Next, the Defendants contend that the Plaintiffs assert claims under state statutes that can only be enforced in connection with consumer transactions, and that these claims must fail because the Plaintiffs have not alleged that the Defendants' allegedly unfair or deceptive conduct was done in the context of a consumer transaction.[219] However, these statutes define "consumers" to include businesses and corporate entities, along with individual consumers.[220] And, many of these statutes also allow for recovery when the unfair or deceptive

---

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

217 *See* Minn. Stat. § 325D.45(1); Neb. Rev. Stat. § 87-303.

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

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

220 *See* Pls.' Br. in Opp'n to Defs.' Mot. to Dismiss, Ex. A-3 [Doc. 471-4].

conduct affected the marketplace as a whole.[221] The Financial Institution Card Issuers constitute "consumers" within the meaning of these statutes because they consumed Equifax's services. Additionally, the Defendants' purportedly unfair or deceptive conduct affected the entire credit reporting marketplace and resulted in injuries to the Financial Institution Card Issuers, which falls within the scope of many of these statutes. Therefore, claims under these statutes should not be dismissed.

Next, the Defendants argue that the Plaintiffs' claims under the Massachusetts Consumer Protection Act should be dismissed because only the Massachusetts Attorney General may bring such actions.[222] However, the text of this statute provides that it is privately enforceable.[223] The Defendants cite Chapter 93H of the Massachusetts General Laws in support of this argument. However, Chapter 93H is a separate statutory scheme regarding security

---

[221] *Id.*

[222] Defs.' Mot. to Dismiss, at 51.

[223] *See* MASS. GEN. LAWS. ch. 93A § 11 ("Any person who engages in the conduct of any trade or commerce and who suffers any loss of money or property, real or personal, as a result of the use or employment by another person who engages in any trade or commerce of an unfair method of competition or an unfair or deceptive act or practice declared unlawful by section two or by any rule or regulation issued under paragraph (c) of section two may, as hereinafter provided, bring an action in the superior court . . . ."). The Defendants cite Section 4 of this Chapter, which merely provides that the Massachusetts Attorney General may bring an enforcement action under this statute. *See* MASS. GEN. LAWS. ch. 93A § 4. This does not preclude private enforcement of the statute, especially given the explicit statutory text providing for such private rights of action.

breaches and the safeguard of personal information.[224] This statute is arguably only enforceable by the Massachusetts Attorney General.[225] Nonetheless, that is irrelevant, since the Plaintiffs assert a claim under Chapter 93A, the Massachusetts Consumer Protection Act. Therefore, the Court finds this argument unpersuasive. Therefore, this argument lacks merit. The Defendants then contend that the Plaintiffs' claim under the Minnesota Plastic Card Act fails.[226] According to the Defendants, this statute only applies to three types of payment card data – CVV codes, PIN numbers, and magnetic strip data.[227] The Defendants contend that the Plaintiff asserting this claim, Firefly Credit Union, fails to allege that the Defendants improperly maintained this data.[228] However, the Court concludes that Firefly has made specific allegations. In the Complaint, Firefly alleges that Equifax retained payment card data, including the card security code, PIN number, and magnetic strip data, longer than allowed by the statute.[229] The Court finds these allegations sufficient.[230]

---

224 *See* MASS. GEN. LAWS. ch. 93H § 2.

225 *See* MASS. GEN. LAWS. ch. 93A § 6.

226 Defs.' Mot. to Dismiss, at 61.

227 *Id.*

228 *Id.*

229 Financial Institution Pls.' Consolidated Am. Compl. ¶ 495.

230 *See* Minn. Stat. § 325E.64(2) ("No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code

H. Payment Card Data

Next, the Defendants contend that the Plaintiffs fail to sufficiently plead claims with regard to payment card data.[231] The Defendants rely primarily upon a recent case from the Seventh Circuit, *Community Bank of Trenton v. Schnuck Markets, Inc.* In *Schnuck*, financial institutions brought suit after a data breach at a grocery store chain resulted in the theft of the data of 2.4 million payment cards.[232] The plaintiffs sued the grocery store, contending that its failure to prevent the data breach, along with its response to the breach, resulted in their injury. The Seventh Circuit ultimately concluded that Illinois and Missouri tort law did not offer "a remedy to card-holders' banks against a retail merchant who suffered a data breach."[233] The court concluded that the economic-loss doctrine precluded tort liabilities for "purely economic losses inflicted by one business on another where those businesses have already ordered their duties, rights, and remedies by contract."[234] And, despite the fact that the plaintiffs had no direct contractual relationship with the defendant, the court nonetheless concluded

---

number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.").

[231] Defs.' Mot. to Dismiss, at 62-64.

[232] *Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 807 (7th Cir. 2018).

[233] *Id.*

[234] *Id.* at 812.

that "[t]he plaintiff banks and Schnucks all participate in a network of contracts that tie together all the participants in the card payment system. That network of contracts imposes the duties plaintiffs rely upon and provides contractual remedies for breaches of those duties."[235] Therefore, the economic loss doctrine precluded the plaintiffs' tort claims.

However, at least at the pleading stage, the Court finds *Schnuck* to be distinguishable. The determinative factor in *Schnuck* was that the financial institutions and retailer were in the same "network of contracts" for payment card systems. In contrast, the Plaintiffs here do not allege that Equifax is part of this "network of contracts." Equifax is not akin to a retailer who is part of this web of a payment card system. In fact, the *Schnuck* court itself acknowledged this distinction, explicitly noting that the Equifax Data Breach presented a fundamentally distinct scenario. The court, citing the instant Equifax Data Breach litigation, noted that "[t]his is also not a situation where sensitive data is collected and then disclosed by private, third-party actors who are not involved in the customers' or banks' direct transactions."[236] It explained that the plaintiffs in that case, as opposed to the Financial Institution Card Issuers here, had existing rights and remedies through the network of contracts, and that they merely sought "additional recovery because they are disappointed by the

---

[235] *Id.* at 814.

[236] *See id.* at 815 (citing *In re Equifax, Inc., Customer Sec. Data Breach Litig.*, 289 F. Supp. 3d 1322 (J.P.M.L. 2017).

reimbursement they received through the contractual card payment systems they joined voluntarily."[237] Thus, the Plaintiffs do not have the type of contractual remedies against the Defendants that the plaintiffs did against the retailer in *Schnuck*. Therefore, the Court finds *Schnuck* inapposite.

I. "Ancillary" Claims

Finally, the Defendants move to dismiss the Plaintiffs' "ancillary claims."[238] First, the Defendants argue that, since the Plaintiffs are not entitled to any substantive relief, they also are not entitled to declaratory relief and cannot recover attorneys' fees. However, as explained above, Financial Institution Card Issuers' claims have been adequately alleged to survive dismissal. Therefore, to the extent that those claims survive, their claims for declaratory relief and attorneys' fees survive. Next, the Defendants contend that the Plaintiffs' claims for equitable relief must be dismissed. According to the Defendants, there are no allegations that the Plaintiffs continue to be harmed by any ongoing conduct by the Defendants.[239] However, the Plaintiffs allege that Equifax's cybersecurity systems remain inadequate, and another breach is

---

237 *Id.*

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

239 *Id.* at 65-66.

imminent.[240] These allegations are sufficient at this stage.[241] Finally, the Defendants contend that the requested injunctive relief is too broad and non-specific.[242] However, at this stage of the litigation, the Plaintiffs state a sufficient claim for injunctive relief. The authority that the Defendants rely upon concerns whether the injunctive order itself is too broad or vague. At this point, the Court is not fashioning the specifics of an injunctive order. Thus, these arguments should not provide the basis for dismissal at this stage. The Court concludes that the Plaintiffs have adequately alleged a claim that they are entitled to injunctive relief.

II. Conclusion

For the reasons stated above, the Defendants' Motion to Dismiss the Financial Institutions' Consolidated Amended Complaint [Doc. 435] is GRANTED in part and DENIED in part. It is GRANTED as to the Financial Institutions and the Associations. It is DENIED as to the Financial Institution Card Issuers.

---

[240] Financial Institution Pls.' Consolidated Am. Compl. ¶¶ 607, 610.

[241] *See In re The Home Depot, Inc. Customer Data Sec. Breach Litig.*, No. 1:14-md-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016) (concluding that the plaintiffs adequately alleged a claim for equitable relief because they "pleaded that the Defendant's security measures continue to be inadequate and that they will suffer substantial harm").

[242] Defs.' Mot. to Dismiss, at 66.

SO ORDERED, this 28 day of January, 2019.

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