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

IN RE: THE HOME DEPOT, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2583 1:14-md-2583-TWT FINANCIAL INSTITUTION CASES

OPINION AND ORDER

This is a data breach case. It is before the Court on The Home Depot, Inc.'s Motion to Dismiss the Financial Institution Plaintiffs' Consolidated Class Action Complaint [Doc. 114], which is GRANTED in part and DENIED in part.

I. Background

Between April 2014 and September 2014, the Defendant, The Home Depot, Inc., was the subject of one of the largest retail data breaches in history.[1] Hackers stole the personal and financial information of approximately 56 million Home Depot customers across the country.[2] The hackers then sold the information on the internet to thieves who made large numbers of fraudulent transactions on credit and debit cards issued to Home Depot customers.[3]

---

1 Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 1.

2 Id.

3 Id.

The Defendant makes a large portion of its sales to customers who use credit or debit cards.[4] Merchants such as the Defendant acquire large amounts of information about each customer when processing card transactions, including the card data and potentially personally identifiable information ("PII") such as financial data and mailing addresses.[5] The Defendant has stored that data in its computer systems for years.[6] In fact, the Defendant stores PII indefinitely.[7] Starting in 2008, the Defendant identified the potential repercussions of a data breach as a risk factor for its business in its annual report and SEC filings.[8]

Despite its acknowledgment of the data security risk, the Plaintiffs allege that the Defendant's data security system suffered from many weaknesses leading up to the data breach at issue here.[9] The weaknesses included failure to maintain an adequate firewall, failure to have adequate internal controls within its computer network, failure to restrict access to cardholder data on its network, failure to use

---

4 Id. ¶ 85.

5 Id. ¶ 88.

6 Id. ¶ 89.

7 Id.

8 Id. ¶ 92.

9 Id. ¶ 96.

coded numbers on its point-of-sale terminals at self checkout lanes, failure to use up-to-date antivirus software on its point-of-sale terminals, failure to encrypt cardholder data at the point of sale, failure to track access to its network, failure to monitor the network for unusual activity, and failure to scan in-store computer systems for vulnerabilities that could be exploited by hackers.[10] The Plaintiffs allege that these failures were due to incompetence by senior management and a desire to cut corners to save money.[11]

The Plaintiffs allege that beginning in 2008, the Defendant's IT employees began reporting data security problems, specifically telling supervisors that the computer systems were "easy prey for hackers" and that they could be breached by anyone with "basic internet skills."[12] Then, starting in 2009, computer experts repeatedly warned the Defendant about the failure to encrypt customer data at the point-of-sale.[13] Without encryption, card data was visible in plain text while being sent from the point-of-sale terminal to the Defendant's main servers, making it vulnerable

---

10 Id.

11 Id. ¶¶ 97-101.

12 Id. ¶ 103.

13 Id. ¶ 104.

to hackers.[14] In 2010, an employee warned the Defendant of a security flaw that allowed unauthorized persons to access the network and navigate freely without triggering any alarms.[15] The Defendant ignored the warnings and fired the employee.[16] Despite warnings from security staffers, the Defendant also failed to properly implement and update antivirus software for its point-of-sale systems.[17] Employees also consistently warned the Defendant about its failure to monitor the network for potential vulnerabilities, abnormalities, and the presence of malware.[18] Furthermore, the Defendant's IT management took affirmative steps to stop employees from fixing security deficiencies and made it known that they would not spend the money to make necessary improvements.[19] Numerous employees working on data security issues left the company beginning in 2011, leaving the IT department understaffed.[20] One of the

---

14 Id.

15 Id. ¶ 105.

16 Id.

17 Id. ¶ 106.

18 Id. ¶ 107.

19 Id. ¶ 109.

20 Id. ¶¶ 118-123.

Defendant's security vendors also threatened to stop working with the company unless it started to take security more seriously.[21]

In the nine months prior to the data breach at issue here, the Defendant had numerous warnings of a problem.[22] In July of 2013, the Defendant suffered a small data breach when hackers placed data-stealing malware on at least eight point-of-sale terminals in a Dallas, Texas, store.[23] In August of 2013, Visa sent a letter warning of an increase in hacker intrusions involving retail merchants.[24] On October 1, 2013, FishNet Security warned the Defendant that its computer systems were vulnerable because the firewall was not operating properly.[25] In December of 2013, the Defendant learned that point-of-sale terminals at one of its stores in Columbia, Maryland, were infected with data-stealing malware that could have been blocked by the proper firewall; the Defendant still failed to upgrade its firewall.[26] Also in December of 2013, hackers installed malware at Target stores nationwide, and the Defendant attempted

---

21 Id. ¶ 123.

22 Id. ¶ 125.

23 Id. ¶ 126.

24 Id. ¶ 127.

25 Id. ¶ 128.

26 Id. ¶ 129.

to respond by assembling a task force to address the situation.[27] In January of 2014, an outside security consultant told the Defendant that its network was vulnerable to attack and did not comply with industry standards.[28] In that same month, the FBI alerted the Defendant about the danger of malware attacks and urged it to update its network security measures.[29] In February of 2014, FishNet again warned the Defendant of the need to upgrade the network's firewall.[30] Also in February of 2014, the data security task force came back with recommendations to improve security; the Defendant did not immediately implement them.[31] Eventually, the Defendant began to implement point-of-sale encryption technology, but by that point, hackers had already infiltrated its computer network.[32]

Beginning in April of 2014, hackers gained access to the Defendant's computer systems using the credentials of a third party vendor, which they were able to do because of the firewall flaw.[33] The hackers were able to freely access the network

---

27 Id. ¶¶ 130-131.

28 Id. ¶ 133.

29 Id. ¶ 134.

30 Id. ¶ 135.

31 Id. ¶¶ 136-37.

32 Id. ¶ 137.

33 Id. ¶ 138.

without triggering any alarms.[34] Inside the network, the hackers targeted the point-of-sale systems at 7,500 self-checkout lanes.[35] They installed malware on those systems that siphoned off the information from a payment card when it was used at a self-checkout lane.[36] The malware remained on the self-checkout terminals until around September 7, 2014.[37] Between September 1, 2014, and September 7, 2014, the credit and debit card information of the Defendant's customers was made available for sale on a black-market website, Rescator.cc.[38]

On September 2, 2014, a security blogger reported that banks were seeing evidence of fraud linked to cards that had made purchases at the Defendant's stores.[39] The U.S. Secret Service also alerted the Defendant that its computer systems had likely been breached.[40] At that point, the Defendant noted that it was looking into the situation, but did not confirm a breach.[41] On September 6, 2014, the Defendant's

---

34 Id. ¶ 139.

35 Id.

36 Id. ¶ 140.

37 Id. ¶ 141.

38 Id. ¶¶ 145-46, 150, 152.

39 Id. ¶ 146.

40 Id. ¶ 148.

41 Id.

investigators confirmed that a security breach had taken place, but did not publicly disclose that information.[42] On September 8, 2014, the Defendant issued a news release that its systems had been breached, but failed to warn that its customers' information was for sale and being used by criminals.[43] On November 6, 2014, the Defendant issued a news release announcing the results of its internal investigation; it admitted that data security should have been a higher priority and that its systems were woefully out of date.[44]

The Plaintiffs here are a putative class of financial institutions that issued and owned payment cards compromised by the data breach,[45] as well as associations of credit unions whose members have been damaged by the data breach.[46] The putative financial institution class alleges that it has been damaged by having to reimburse customers for the fraud losses suffered due to the data breach as well as by other costs such as having to reissue payment cards. The putative class brings claims for negligence and negligence per se, as well as violation of eight state-specific consumer

---

42 Id. ¶ 151.

43 Id. ¶ 154.

44 Id. ¶¶ 158-59.

45 Id. ¶¶ 11-61.

46 Id. ¶¶ 62-80.

protection statutes. The putative class also seeks injunctive and declaratory relief. The association plaintiffs do not sue as a class.[47] They seek only equitable relief. The Defendant moves to dismiss all the claims by both the putative class and the association plaintiffs.

II. Legal Standard

A complaint should be dismissed under Rule 12(b)(6) only where it appears that the facts alleged fail to state a "plausible" claim for relief.[48] A complaint may survive a motion to dismiss for failure to state a claim, however, even if it is "improbable" that a plaintiff would be able to prove those facts; even if the possibility of recovery is extremely "remote and unlikely."[49] In ruling on a motion to dismiss, the court must accept the facts pleaded in the complaint as true and construe them in the light most favorable to the plaintiff.[50] Generally, notice pleading is all that is required for a valid

---

47 Id. ¶ 62.

48 Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009); Fed. R. Civ. P. 12(b)(6).

49 Bell Atlantic v. Twombly, 550 U.S. 544, 556 (2007).

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

complaint.[51] Under notice pleading, the plaintiff need only give the defendant fair notice of the plaintiff's claim and the grounds upon which it rests.[52]

III. Discussion

A. Standing

The Defendant first moves to dismiss all of the Plaintiffs' claims for lack of standing. 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."[53] The Supreme Court has held that "threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient."[54] 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."[55] Here, the financial institution plaintiffs have adequately pleaded

---

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

[52] See Erickson v. Pardus, 551 U.S. 89, 93 (2007) (citing Twombly, 550 U.S. at 555).

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

[54] Id.

[55] Id. at 1150 n.5.

standing. 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.[56] These injuries are not speculative and are not threatened future injuries, but are actual, current, monetary damages. Additionally, any costs undertaken to avoid future harm from the data breach would fall under footnote 5 of Clapper, specifically as reasonable mitigation costs due to a substantial risk of harm. The injuries, as pleaded, are also fairly traceable to Home Depot's conduct, specifically the alleged failure to implement adequate data security measures. A favorable ruling would also redress these monetary harms. The Defendant's motion to dismiss for lack of standing should be denied.

B. Negligence and Negligence Per Se

Next, the Defendant argues that the Plaintiffs' negligence and negligence per se claims are barred by the economic loss rule. "The 'economic loss rule' generally provides that a contracting party who suffers purely economic consequences must seek his remedy in contract and not in tort."[57] In other words, "a plaintiff may not

---

[56] Financial Inst. Pls.' Consolidated Class Action Compl. ¶¶ 186-191.

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

recover in tort for purely economic damages arising from a breach of contract."[58] 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."[59] Here, even though there is a contract between the card issuers and the Plaintiffs, the independent duty exception would bar application of the economic loss rule. Georgia recognizes a general duty "to all the world not to subject them to an unreasonable risk of harm."[60] A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort.[61] Here, the Plaintiffs have pleaded that the Defendant knew about a substantial data security risk dating back to 2008 but failed to implement reasonable security measures to combat it.[62] This

---

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

[59] 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).

[60] Bradley Center, Inc. v. Wessner, 250 Ga. 199, 201 (1982).

[61] In re Target Corp. Cust. Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1310 (D. Minn. 2014) (ruling on motion to dismiss in financial institution cases).

[62] Financial Inst. Pls.' Consolidated Class Action Compl. ¶¶ 205-06.

Court therefore finds that an independent duty existed, barring application of the economic loss rule.

The Court declines the Defendant's invitation to hold that it had no legal duty to safeguard information even though it had warnings that its data security was inadequate and failed to heed them. 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. The Defendant's motion to dismiss based on the economic loss rule should be denied. Additionally, the Defendant moves to dismiss the Plaintiffs' negligence claim on the ground that it owed no duty to the Plaintiffs. Because this Court finds that a duty does exist, the motion to dismiss on the ground that there was no duty should also be denied.

The Defendant also moves to dismiss the Plaintiffs' negligence per se claim. "Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se."[63] 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

---

[63] Pulte Home v. Simerly, 322 Ga. App. 699, 705 (2013).

the harm suffered.[64] Here, the Plaintiffs allege that Home Depot violated Section 5 of the FTC Act. The Defendant argues that Section 5 cannot form the basis of a negligence per se claim. The Consolidated Class Action Complaint here adequately pleads a violation of Section 5 of the FTC Act, that the Plaintiffs are within the class of persons intended to be protected by the statute, and that the harm suffered is the kind the statute meant to protect.[65] 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.[66] The Defendant's motion to dismiss the negligence per se claim should be denied.

C. Injunctive and Declaratory Relief

Next, the Defendant moves to dismiss the Plaintiffs' claim for Injunctive and Declaratory Relief. First, the Defendant argues that the Plaintiffs are pursuing an impermissible standalone claim for injunctive relief and impermissibly requesting an injunction related to a negligence claim. Not so. Instead, the Plaintiffs ask for an

---

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

65 Financial Inst. Pls.' Consolidated Class Action Compl. ¶¶ 217, 219-20.

66 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).

injunction corresponding to their declaratory judgment claim.[67] Such a claim is permissible under the Declaratory Judgment Act.[68]

The Defendant next argues that the Plaintiffs' claim for injunctive and declaratory relief is based on a speculative future data breach. The Supreme Court has held that there must be "a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment."[69] The Plaintiffs have pleaded that the Defendant's security measures continue to be inadequate and that they will suffer substantial harm.[70] The Plaintiffs have pleaded sufficient facts to survive a motion to dismiss regarding a future breach. The Defendant next argues that the Plaintiffs have an adequate remedy at law. Contrary to the Defendant's argument, the Plaintiffs do allege that they will lack an adequate legal remedy if another breach occurs.[71] The Defendant's motion to dismiss the claim for injunctive relief on remedy grounds should be denied.

---

67 Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 281.

68 28 U.S.C. § 2202 ("Further necessary or proper relief based on a declaratory judgment or decree may be granted."); Powell v. McCormack, 395 U.S. 486, 499 (1969) ("A declaratory judgment can then be used as a predicate to further relief, including an injunction.").

69 MedImmune v. Genentech, Inc., 549 U.S. 118, 127 (2007).

70 Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 279.

71 Id. ¶ 282.

The Defendant then argues that the Plaintiffs' claim for declaratory relief seeks an impermissible determination of past liability. "Declaratory relief is appropriate when it is necessary to 'protect the plaintiff from uncertainty and insecurity with regard to the propriety of some future act or conduct.'"[72] The Plaintiffs ask for a declaration that the Defendant "breached and continues to breach" its duty.[73] As to the claim for declaratory relief that the Defendant already breached its duty, the Defendant's motion to dismiss should be granted because that deals with past liability and is properly covered under the Plaintiffs' negligence claims. As to the continuing nature of the breach, however, the Defendant's motion to dismiss should be denied.

Finally, the Defendant argues that the association plaintiffs do not have standing to bring a claim for declaratory relief because participation of the individual members of the associations is required. "It is well-established that an association may seek equitable relief on behalf of its members without running afoul of the [member participation requirement]."[74] Here, the association plaintiffs are seeking only

---

[72] Tiller v. State Farm Mut. Auto. Ins. Co., No. 1:12-cv-3432-TWT, 2013 WL 451309, at *3 (N.D. Ga. Feb. 5, 2013) (quoting Henderson v. Alverson, 217 Ga. 541 (1962)), aff'd, 549 F. App'x 849 (11th Cir. 2013).

[73] Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 280.

[74] In re Managed Care Litig., 298 F. Supp. 2d 1259, 1308 (S.D. Fla. 2003) (citing Hunt v. Washington State Apple Advert. Comm., 432 U.S. 333, 343 (1977)).

equitable relief. The participation of individual members is therefore not required. The Defendant's motion to dismiss the association plaintiffs should be denied.

D. State Law Claims

The Defendant also moves to dismiss the Plaintiffs' state statutory claims. First, the Defendant argues that the Plaintiffs do not have standing to bring these claims. As discussed above, this Court finds that the Plaintiffs do have standing. The Plaintiffs make claims as subclasses based on states of residence under eight separate state statutes.

1. Alaska

The Defendant first argues that the Plaintiffs have not pleaded an unfair act under Alaska Stat. Ann. § 45.50.471(b). That statute gives an illustrative, but not exhaustive list of unfair acts.[75] Alaska looks to the FTC Act and federal law for guidance in interpreting the meaning of unfair acts or practices.[76] The Defendant first argues that because maintaining inadequate security measures is not listed as an unfair act in the statute, the Plaintiffs' claim must be dismissed. Given that the statute specifically makes its list of unfair acts illustrative but not exhaustive, this argument

---

[75] Alaska Stat. Ann. § 45.50.471(b) ("The terms 'unfair methods of competition' and 'unfair or deceptive acts or practices' include, but are not limited to . . .").

[76] State v. O'Neill Investigations, Inc., 609 P.2d 520, 535 (Alaska 1980).

must fail. Additionally, courts have found that it can constitute an unfair practice under the FTC Act to maintain inadequate security measures.[77] The Plaintiffs allege that the Defendant failed to maintain adequate security measures.[78] The Defendant's motion to dismiss the Plaintiffs' claim under Alaska Stat. Ann. § 45.50.471(b) should be denied.

2. California

The Defendant moves to dismiss the Plaintiffs' claims under California's Unfair Competition Law ("UCL") and Customer Records Act ("CRA"). The complaint first pleads that the Defendant violated the CRA. That statute, however, may only be asserted by customers – individuals "who provide[] personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business."[79] The Plaintiffs here do not fall within that definition because they did not obtain products or services from the Defendant. The standalone claim under the CRA should be dismissed.

---

[77] See, e.g., In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496 (1st Cir. 2009).

[78] Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 224.

[79] Cal. Civil Code §§ 1798.84(b), 1798.80(c).

The Plaintiffs also assert a claim under the UCL. The UCL prohibits "any unlawful, unfair or fraudulent business act."[80] Here, the Plaintiffs have pleaded a violation of the "unfair" prong of the statute by pleading that the Defendant failed to maintain adequate and reasonable security measures and that its conduct undermined California public policy.[81] The unlawful prong of the UCL prohibits "anything that can properly be called a business practice and that at the same time is forbidden by law."[82] Here, the Plaintiffs have properly pleaded a CRA violation to satisfy the "unlawful" prong of the UCL.[83] It does not matter that the CRA does not provide the Plaintiffs with a private cause of action because the UCL "can form the basis for a private cause of action even if the predicate statute does not."[84] The Defendant's motion to dismiss the UCL claim should be denied.

3. Connecticut

---

80 Cal. Bus. & Prof. Code § 17200.

81 Financial Inst. Pls.' Consolidated Class Action Compl. ¶¶ 232-34.

82 Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co., 973 P.2d 527, 539 (Cal. 1999).

83 Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 235.

84 Chabner v. United of Omaha Life Ins. Co., 225 F.3d 1042, 1048 (9th Cir. 2000).

The Defendant moves to dismiss the Plaintiffs' claim under the Connecticut Unfair Trade Practices Act ("CUTPA"). As a threshold matter, the Defendant argues that the Plaintiffs have failed to plead an unfair trade practice, but as discussed with the Alaska statute, that is not the case. The Defendant next argues that this claim fails because no duty exists between the Defendant and the Plaintiffs. As discussed above, this Court finds that the Defendant did owe the Plaintiffs a duty. Finally, the Defendant argues that the CUTPA claim is based on mitigation damages that are not the proximate result of the Defendant's conduct. As discussed above, this Court finds that the Plaintiffs have pleaded damages proximately caused by the Defendant. The Defendant's motion to dismiss the CUTPA claim should be denied.

4. Florida

The Defendant also moves to dismiss the Plaintiffs' claim under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"). Businesses are only authorized to bring actions under FDUTPA if they are acting as consumers by engaging in the purchase of goods or services from the defendant.[85] The complaint here does not allege that the Plaintiffs were engaging in the purchase of goods or services from the Defendant. Nor does this Court believe that the action of the banks

[85] Carroll v. Lowes Home Centers, Inc., No. 12-23996-CIV, 2014 WL 1928669, at *4 (S.D. Fla. May 6, 2014).

in issuing credit and debit cards to the individual consumers could be construed as purchasing goods or services. The motion to dismiss the FDUTPA claim should be granted.

5. Illinois

The Defendant moves to dismiss the claim under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"). The Defendant argues that the Plaintiffs have not alleged the sort of conduct required for a deceptive or unfair practice claim under that statute. Addressing a data breach at another national retailer, the Northern District of Illinois found that where a plaintiff alleged failure to comply with industry standards, that plaintiff could survive a motion to dismiss a claim under ICFA.[86] That is exactly what the Plaintiffs have alleged here.[87] The motion to dismiss the ICFA claim should be denied.

6. Massachusetts

The Defendant moves to dismiss the claim under the Massachusetts Consumer Protection Act ("MCPA"). Again the Defendant argues that the Plaintiffs have failed to allege conduct within the scope of the statute. Applying Massachusetts law, the

---

[86] In re Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 525-526 (N.D. Ill. 2011).

[87] Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 249.

First Circuit found that the type of inadequate data security measures alleged by the Plaintiffs here are sufficient to survive a motion to dismiss under the MCPA.[88] The motion to dismiss the MCPA claim should be denied.

7. Minnesota

The Defendant moves to dismiss the claim under the Minnesota Plastic Card Security Act ("MPCSA"). That statute prohibits persons and entities conducting business in Minnesota from retaining certain financial data for more than 48 hours after a card transaction.[89] The Plaintiffs allege that the Defendant kept payment card data for more than 48 hours after authorization, exactly what the MPCSA prohibits.[90] The motion to dismiss the MPCSA claim should be denied.

8. Washington

The Defendant moves to dismiss the claims under Wash. Rev. Code Ann. § 19.255.020 and the Washington Consumer Protection Act. The Defendant states that § 19.255.020 exempts companies from liability if they were certified compliant with the payment card industry data security standards ("PCI-DSS") within a year of the breach and argues that because it was certified compliant, it cannot be held liable. The

---

[88] In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496 (1st Cir. 2009).

[89] Minn. Stat. Ann. § 325E.64.

[90] Financial Inst. Pls.' Consolidated Class Action Compl. ¶ 265.

Defendant then argues that because the Plaintiffs rely on the violation of § 19.255.020 to prove a violation of the Washington Consumer Protection Act, that claim should be dismissed as well. What the Defendant fails to note, however, is that the Plaintiffs allege that it was *not* in compliance with PCI-DSS standards at the time of the data breach.[91] The Defendant's argument fails and the motion to dismiss the claims under the Washington statutes should be denied.

E. Ripeness

Finally, the Defendant argues that the Plaintiffs' claims are not ripe because of the ongoing card brand recovery process, which could potentially reimburse the Plaintiffs for some of their losses. A claim is ripe if the controversy is "definite and concrete, touching the legal relations of parties having adverse legal interests."[92] The claim here is one for damages related to past conduct. That is certainly definite and concrete. This Court finds no need to wait any longer to resolve this claim. Although the Defendant might be entitled to reduce any damages it may have to pay based on the card brand recovery process, this is no reason to dismiss this litigation based on ripeness. It is also worth noting that the Plaintiffs do not mention the card brand

---

[91] Id. ¶¶ 173-75, 178.

[92] Aetna Life Ins. Co. of Hartford, Conn. v. Haworth, 300 U.S. 227, 240-41 (1937).

recovery process in their complaint, so this Court declines to consider it as a basis for granting a motion to dismiss, which is to be decided only on the basis of the four corners of the complaint. The motion to dismiss based on ripeness should be denied.

IV. Conclusion

For the reasons stated above, The Home Depot, Inc.'s Motion to Dismiss the Financial Institution Plaintiffs' Consolidated Class Action Complaint [Doc. 114] is GRANTED in part and DENIED in part.

SO ORDERED, this 17 day of May, 2016.

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