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	)	Case No.: 1:14-md-02583-TWT
This document relates to:	)	
CONSUMER CASES	)	

CONSUMER PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO HOME DEPOT'S MOTION TO DISMISS THE COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

INTRODUCTION

"***We sell hammers***." That is how Home Depot management repeatedly responded when its skeleton crew of IT security personnel implored them to implement long overdue, industry-standard security measures. Ignoring those recommendations led directly to one of the largest data breaches in history—a breach that compromised the personal and financial information of 56 million individuals. For years, Home Depot put the bottom line ahead of its customers' security by understaffing its information technology ("IT") security department, ignoring security recommendations made by IT employees and consultants, and hiring unqualified managers to serve in key positions. The data breach was not only foreseeable, but actually forecasted by Home Depot employees. Consequently, millions of customers suffered harm, including fraud and identity theft. Many more are at a substantial risk of future harm. Home Depot's characterization of the harm suffered by the Consumer Plaintiffs ("Plaintiffs") as "intangible" or mere "annoyances and inconveniences" ignores the detailed allegations of the Complaint and tries to discredit the millions of people who not only had their lives interrupted, but also suffered real and severe consequences as a direct result of Home Depot's refusal to implement and follow proper security protocols. Home Depot's motion to dismiss should be denied in its entirety.

BACKGROUND

Home Depot's data security failures are years in the making. Dating back to 2002, it made record investments in technology aimed at boosting sales without

making corresponding investments in data security. *See* Consolidated Class Action Complaint (Doc. 93) ("Complaint" or "Compl."), ¶¶ 106-09. In 2008, Home Depot identified a data security breach as a "risk factor" in its annual SEC filings and report to shareholders, but undertook no efforts to actually minimize the emerging risk. *Id*., ¶ 110. That same year, Home Depot hired Matthew Carey as its new Chief Information Officer. *Id*., ¶ 113. Under Carey's leadership, the company's information technology focus was on software development and IT infrastructure to support sales, not data security. *Id*., ¶¶ 114, 135. For instance, Carey oversaw the implementation of Motorola handheld devices known as "First Phones." *Id*., ¶¶115-16. Starting in 2010 and continuing through March 2011, an employee warned of major security vulnerabilities in First Phones that permitted unauthorized access into Home Depot's computer network. *Id*., ¶119. Rather than heed the employee's explicit warnings, Home Depot terminated the employee. *Id*., ¶ 131. This action reflected the culture at Home Depot related to data security.

In 2011, Carey appointed Jeff Mitchell as the new Chief Information Security Officer (CISO). Acting on Carey's orders to cut costs, Mitchell eliminated a number of essential security programs and protocols. *Id*., ¶¶ 135-140. Mitchell's bullying management style was so polarizing that within three months of his taking over as CISO, approximately half of Home Depot's 60 IT security employees departed. *Id*., ¶ 137. When those who remained raised concerns about data security, they were ignored or bullied into silence. *Id*., ¶¶ 118, 131. Prior to the data breach,

employees cautioned that it was "painfully easy" to capture data from the company's network and some even warned friends to use cash, rather than credit cards, at Home Depot retail stores. *Id*., ¶¶ 150, 152. The frustrations of employees and third-party security vendors were perhaps best epitomized by the phrase they repeatedly heard from management in response to requests for new software and training: "*We sell hammers*." *Id*., ¶ 157.

In approximately April 2014, hackers gained access to and took control of Home Depot's data systems by using the credentials of a third-party vendor. Once inside, the hackers installed data-stealing malware on Home Depot's self-checkout terminals. *Id*., ¶¶ 176-79. The breach went undetected for almost six months, and was only discovered after the cyber-thieves began selling massive quantities of customers' financial information over the Internet. *Id*., ¶¶ 82, 184-85. The stolen information included debit and credit card numbers, expiration dates, three-digit security codes, and customers' names, mailing addresses and ZIP codes. Phone numbers and e-mail addresses were also stolen. *Id*., ¶ 199. Purchasers of the stolen data had access to so much information they were able to make fraudulent purchases, fabricate new PIN numbers for stolen debit cards in order to withdraw cash from ATMs, and extract customers' Social Security numbers and dates of birth by using services widely available on the Internet. *Id*., ¶¶ 204-05. The breadth of compromised information permitted criminals to commit any number of frauds,

many of which are detailed in the Complaint, and only a sampling of which are summarized below:

a. Fraudulent charges of $8,500, repeated attempts at identity theft resulting in a seven-year freeze placed on credit reports with all three credit bureaus, monthly payments for credit monitoring, and 320 hours of time and effort (¶ 4);

b. Identity theft resulting in a $10,000 line of credit being opened in another state and a lowered credit score triggering the denial of refinancing efforts for a home mortgage (¶ 5);

c. Lost access to a line of credit for several weeks and victim of multiple attempts of identity theft (¶ 6);

d. Fraudulent charges and overdrawn account; forced to borrow money to pay bills while waiting for charges to be reversed (¶ 7);

e. Thousands of dollars in fraudulent charges, overdrawn account, overdraft penalty fees, temporary spending limits imposed on accounts and missed meals because of no access to funds (¶ 8);

f. Fraudulent purchases using fake credit card made with plaintiff's information; denied credit as a result of fraudulent activity on credit report; monthly fees for credit monitoring (¶ 9);

g. Account frozen after fraudulent activity identified; stranded without access to funds; six fraudulent credit applications appearing on plaintiff's credit reports; auto-insurance policy cancelled after freeze on plaintiff's bank account prevented timely automatic payment; borrowed money to pay bills (¶ 10);

h. Fraudulent purchases and ATM withdrawals on debit account totaling $1,800; account frozen; forced to use alternative funding sources to cover the stolen funds (¶ 35);

i. Fraudulent charges; account frozen for 10 days; missed 20 automatic bill payments tied to compromised accounts; lowered line of credit (¶ 86).

In each case, Plaintiffs spent hours of their time dealing with repercussions of the data breach. While Home Depot tries to characterize these claims as "dependent on the hypothetical future acts of third parties,"—in reality, this harm was the inevitable and predictable result of Home Depot's indifference to data security. Indeed, prior to the breach, Home Depot management refused to implement essential data security measures, many of which had been proposed by IT employees and outside security consultants for years. *See id*., ¶ 220. Had Home Depot adopted any of these measures, the breach would not have been possible or would have been mitigated through early detection. *Id*. To make matters worse, Home Depot's delayed and uninformative notifications about the security breach directly resulted in millions of more individuals suffering harm. *Id*., ¶ 222. Former CEO Francis Blake even conceded his company's data security failures: "***If we rewind the tape, our security systems could have been better. Data security just wasn't high enough in our mission statement***." *Id*., ¶ 224.

Plaintiffs assert class action claims against Home Depot for violations of state consumer protection statutes (Count I); violations of state data breach notification statutes (Count II); negligence (Count III); breach of implied contract (Count IV); unjust enrichment (Count V); declaratory judgment (Count VI); violations of the California Customer Records Act, California Civil Code § 1798.81.5 and the California Unfair Competition Law's unlawful prong (Count VII); and violations of the Maryland Personal Information Protection Act and

Consumer Protection Act, Maryland Code Commercial Law §§ 13-101 *et seq*., 14-3501 *et seq*. (Count VIII). Plaintiffs request monetary relief, including actual and statutory damages, restitution, and disgorgement, and injunctive relief requiring Home Depot to implement and maintain adequate security measures.

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." *RLI Ins. Co. v. Banks*, No. 1:14-CV-1108-TWT, 2015 WL 400540, at *1 (N.D. Ga. Jan. 28, 2015) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009)). A claim may survive even where recovery is "improbable," or "remote and unlikely." *Id*. (quoting *Bell Atl. v. Twombly*, 550 U.S. 544, 556 (2007)). Even after *Twombly* and *Iqbal*, "notice pleading is all that is required for a valid complaint." *Id*. Through their detailed Complaint, Plaintiffs readily meet this standard.

ARGUMENT

I. Plaintiffs Have Article III Standing to Sue

To establish Article III standing, "an injury must be concrete, particularized, and actual *or* imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Intern. USA*, 133 S.Ct. 1138, 1147 (2013) (emphasis added). Plaintiffs establish that they have Article III standing by documenting the economic and non-economic injuries they already have suffered, establishing the substantial risk of future harm, tying their injuries to Home Depot's conduct, and explaining the remedies the Court can provide.

In its brief in support of its Motion to Dismiss (Doc. 105-1) ("Mtn."), Home Depot argues that not one of the 85 named Plaintiffs suffered injury sufficient to confer Article III standing. To make this argument, Home Depot *mischaracterizes* the various harms alleged by Plaintiffs. For example, Home Depot refers to a Plaintiff dealing with the repercussions of having a fraudulent tax return filed in his name as "the inconvenience of having to file paper." Mtn. at 29.[1] Those Plaintiffs who took necessary mitigation measures like purchasing credit monitoring or freezes are condemned as creating "self-inflicted injuries." Mtn. at 30. Even those Plaintiffs with out-of-pocket money damages are chastised because they did not allege "why their banks or other vendors failed to reimburse fees that plainly should have been reimbursed." Mtn. at 35.

Along the way, Home Depot manages to place blame on "the independent actions of criminals" (Mtn. at 35), "banks and other vendors who refused to reimburse" unauthorized charges on Plaintiffs' accounts (Mtn. at 34), and even "*plaintiffs* themselves" (Mtn. at 41). But Home Depot's blame-shifting is not a fair characterization of the Complaint. Plaintiffs allege in great detail their injuries flowing from the data breach, including fraudulent charges made to their payment cards following the black market sale of their stolen data. Such injuries constitute not just imminent—but *actual*—injuries-in-fact, which were the foreseeable result of, and fairly traceable to, Home Depot's failure to implement adequate security

[1] Citations to page numbers refer to the ECF page numbers in the top right-hand corner of all electronic filings.

measures. The Court may redress these injuries by awarding damages and equitable relief.

A. All Plaintiffs Suffered Justiciable Injury from Home Depot's Unlawful Conduct

The injury component of Article III standing is satisfied by allegations of *either* "actual or imminent" injury. *Clapper*, 133 S. Ct. at 1147. Here, Plaintiffs allege actual *and imminent* injuries, including: (1) theft of credit or debit account and personal information (Compl., ¶¶ 2, 96, 261, 289); (2) unauthorized and unreimbursed charges and fees on their payment card accounts (*id*., ¶¶ 2, 261, 289); (3) frozen accounts, which forced them to incur late payment fees, borrow money to meet living needs, and damaged their credit (*id*., ¶¶ 2, 100, 261, 289); and (4) costs associated with the detection and prevention of identity theft, including purchasing credit monitoring services (*id*., ¶¶ 2, 261, 289), among other injuries (*see id*. ¶¶ 2, 97, 261, 289).

1. General Principles of Injury for Article III Standing

Home Depot's standing argument is predicated on a strained interpretation of *Clapper*. In *Clapper*, the ACLU sought a declaratory judgment to halt new provisions of a federal statute that allowed the NSA to monitor certain communications. Notably, the ACLU filed suit before the challenged surveillance began. 133 S. Ct. 1138. Not surprisingly, the Supreme Court held that the plaintiffs lacked standing to challenge the program because they "fail[ed] to offer any evidence that their communications have been monitored." *Id.* at 1148.

Clapper does not represent a sea change in standing jurisprudence or immunize companies from liability for negligence. Rather, *Clapper* merely confirms that where standing is based on a "threatened injury," that injury "must be *certainly impending* to constitute injury in fact" and "allegations of *possible* future injury are not sufficient." 133 S. Ct. at 1147 (citations omitted). In fact, *Clapper* endorsed finding standing "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Id.* at n.5 (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153 (2010)).

This case is not like *Clapper*. First, it does not implicate national security or separation of power concerns, which require "especially rigorous" standing analyses. *Id.* at 1147. Second, this case does not involve the "highly attenuated chain of possibilities" presented in *Clapper*. *Id.* at 1148. Plaintiffs' information *already* has been sold in massive quantities over the Internet and class members *already* have suffered concrete injuries, including actual financial losses. Plaintiffs also face real, concrete and "certainly impending" continued threats stemming from the sale of their personal information. In fact, the Supreme Court recently reaffirmed that harm having already occurred is "good evidence" of future harm. *See Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2345 (2014) (distinguishing *Clapper* on this basis).

This case is more akin to *Monsanto*, where the Supreme Court held that a bee's anticipated pollination patterns create a sufficiently imminent risk of injury to farmers who feared gene flow from genetically modified plants planted in nearby fields. 561 U.S. 139. Faced with similar facts, lower courts also have consistently recognized Article III standing, even where, unlike here, no actual misuse of compromised information has occurred. *See, e.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) ("injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions"); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010) (plaintiffs "whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III"). Likewise here, Plaintiffs who stand to suffer future injuries have standing to sue.

2. Analysis of Standing in Data Breach Cases

As Home Depot acknowledges, the Eleventh Circuit has found that an injury in fact occurs when "Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 (11th Cir. 2012). In *AvMed*, criminals opened financial accounts in the plaintiffs' names and then made fraudulent charges or overdrew the accounts. *Id.* The court held that allegations of monetary injury were sufficient to confer standing. *Id.* Other courts have held that similar allegations conferred standing in data breach cases. For example, in *In re Target Corp. Data Sec. Breach*

Litig.,[2] which dealt with facts and claims almost identical to this case, the court swiftly disposed of the argument that consumers did not allege sufficient injury:

> Plaintiffs have alleged injury. Indeed, [the Complaint recites] many of the individual named Plaintiffs' injuries, including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees. Target ignores much of what is pled, instead contending that because some Plaintiffs do not allege that their expenses were unreimbursed or say whether they or their bank closed their accounts, Plaintiffs have insufficiently alleged injury. These arguments gloss over the actual allegations made and set a too-high standard for Plaintiffs to meet at the motion-to-dismiss stage. Plaintiffs' allegations plausibly allege that they suffered injuries that are "fairly traceable" to Target's conduct.

Target, at *2. Other courts analyzing data breach cases post-*Clapper* agree.[3] For example, the *Sony* court found that "Plaintiffs' allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [were] sufficient to establish Article III standing at this stage in the proceedings." 996 F. Supp. 2d at 962. Likewise, in *Adobe*, hackers accessed the personal information of at least 38 million customers, including names, credit and debit card numbers, expiration dates and mailing and email addresses. 2014 WL 4379916 at *2. The court found that "the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*" because "the risk that

---

[2] No. MDL 14-2522 PAM/JJK, 2014 WL 7192478 (D. Minn. Dec. 18, 2014).

[3] *See*, *e.g*., *In re Sony Gaming Networks and Customer Data Breach Security Litig*. ("*Sony II*"), 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014); *In re Adobe Systems, Inc. Privacy Litig*. ("*Adobe*"), No. 13-CV-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014).

Plaintiffs' personal data will be misused by the hackers . . . is immediate and very real." *Id.* at *8. There, as here, speculation was not required as "stolen data had already surfaced on the internet." *Id.* Accordingly "the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as 'certainly impending'" and "the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused." *Id*. *See also Moyer v. Michaels Stores, Inc.*, No. 14-C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014) ("elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent").

3. Fraudulent Charges, Mitigation Costs and Time Spent Addressing the Data Breach Are Article III Injuries

Home Depot attempts to distinguish between fraudulent charges to Plaintiffs' credit and debit cards and "identity theft" to argue that identity theft is too "speculative" of an injury under *Clapper*. This is a distinction without a difference because fraudulent charges are a form of identity theft. *See, e.g.*, 18 U.S.C. §§ 1029, 1344 (criminalizing identity theft involving misuse of payment cards). Moreover, Plaintiffs specifically allege that thieves were able to leverage the data obtained through the data breach to acquire additional information—including extracting customers' Social Security numbers and dates of birth using services widely available on the Internet. *Id*., ¶¶ 204, 205. Under these circumstances, Plaintiffs' future injuries are not "too speculative."

Home Depot writes off other injuries suffered by Plaintiffs, including the nearly 2,000 hours that the named Plaintiffs spent curing problems from the breach, as mere "annoyance and inconvenience." Mtn. at 17-18. But such injuries are real, immediate and non-speculative. *See F.T.C. v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602, 625 (D.N.J. 2014) (finding data breach has potential to cause "substantial injury" to consumers). The extensive efforts undertaken by Plaintiffs directly flowed from the breach and are therefore compensable damages.

Home Depot also downplays the injuries of those who experienced fraudulent charges by relying on extrinsic evidence to argue that most card issuers have "zero liability" policies that reimburse customers for unauthorized charges (*see* Mtn. at 20, n. 6). But in *AvMed*, the Eleventh Circuit rejected the argument that standing should hinge on whether losses are "reimbursed." *See AvMed*, 693 F.3d at 1324 ("AvMed contends that Plaintiffs' injuries are not cognizable under Florida law because the Complaint alleges only 'losses,' not 'unreimbursed losses.' This is a specious argument."). Moreover, under federal law, consumers *can be liable* for fraudulent charges on their credit cards of up to $50, and potentially much more in the case of fraudulent charges to debit cards—up to the full amount in the account. *See* 15 U.S.C. § 1643 (credit cards); 15 U.S.C. § 1693g (debit cards). These are actual injuries, supported by federal laws and guidelines.

Home Depot also asserts that certain Plaintiffs tried to "create standing" with "self-inflicted injuries" by taking mitigation measures like purchasing credit

freezes or monitoring. But *Clapper* recognized that in cases where there is a substantial risk harm will occur, plaintiffs may be prompted "to reasonably incur costs to mitigate or avoid that harm." *Clapper*, at 1150 n.5 (citing *Monsanto*, 561 U.S. at 153-54). *See also Adobe*, at *9 ("costs incurred in an effort to mitigate the risk of future harm [] constitute injury-in-fact"); *Anderson v. Hannaford Bros. Co*., 659 F.3d 151, 164 (1st Cir. 2011) (where plaintiffs face imminent harm,"[t]he question then becomes whether plaintiffs' mitigation steps were reasonable."). Plaintiffs acted reasonably in trying to remedy, limit, and prevent the vast array of injuries described above.

Finally, Home Depot argues that its offer of limited free credit monitoring renders Plaintiffs' purchases of similar products unnecessary. This unsupported argument ignores the Complaint's factual allegations that numerous Plaintiffs were never made aware of Home Depot's offer of credit monitoring. *See id*., ¶ 201. Moreover, common sense dictates that many class members were likely skeptical of again relying on Home Depot to protect their personal information. Plaintiffs' mitigation costs, as alleged, were reasonable and constitute injury-in-fact.

4. Home Depot's Cited Authority is Unpersuasive

With little analysis, Home Depot cites to a number of cases to argue that Plaintiffs' allegations of injury are insufficient to confer standing.[4] But a closer examination of these cases demonstrates their limited value here. For instance, in

[4] *See* cases cited in Mtn. at 25-27.

Galaria v. Nationwide, 998 F. Supp. 2d 646 (S.D. Ohio 2014), hackers obtained customers' personal information (though not credit card information) from the servers of an insurance company. The court declined to find standing based on increased risk of future harm, reasoning that whether plaintiffs would be harmed depended on the decision of the unknown hackers. *Id*. at 656. Addressing this argument in *Adobe*, the court dismissed the reasoning of *Galaria* as "unpersuasive" and declined to follow it because "after all, why would hackers target and steal personal customer data if not to misuse it?" *Adobe*, at *9. The *Adobe* court further found that "*Galaria's* reasoning lacks force" in cases like this "where Plaintiffs allege that some of the stolen data has already been misused." *Id*.

In re Science Apps. Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014), did not involve a targeted data breach at all. Rather, a thief broke into a car and stole a GPS and stereo, together with encrypted backup data tapes containing personal medical information of four million military members. *See id*. at 19. The thief would not have been able to misuse the data without an attenuated chain of events, including the thief realizing what he stole. *Id.* at 24. This "accidental" theft of sensitive data is fundamentally different than the intentional hacking of payment systems. *See Adobe*, at *9 (distinguishing *SAIC* and noting that "hackers targeted Adobe's servers in order to steal customer data"). Similarly, in *Barnes & Noble Pin Pad Litig*.,[5] the plaintiffs did not clearly allege

[5] No. 12–8617, 2013 WL 4759588, at *4 (N.D. Ill. Sep. 3, 2013).

that the plaintiffs' information was taken for misuse. *Cf. Adobe*, at *9 (distinguishing *Barnes & Noble* because "it was unclear if the plaintiffs' information had been taken at all"). And in *Remijas v. Neiman Marcus Group, LLC*, the district court noted that "the overwhelming majority of the plaintiffs allege only that their data *may* have been stolen,"[6] an allegation not present here.

In a similar vein, the plaintiffs in *Lewert v. P.F. Chang's China Bistro, Inc.*,[7] did "not allege that any fraudulent charges were made to the debit card he used at P.F. Chang's," only that "the charges were either declined or attempted." *Id*. at *2. Home Depot cites to another case from that district, *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 881 n.18 (N.D. Ill. 2014), but that plaintiff "concede[d] that she has not sought or received any notice . . . that her PII was compromised by the breach." Another court within the same district has declined to follow *Trustwave's* over-aggressive view of *Clapper*. *See Moyer*, 2014 WL 3511500 at *5 (comparing data breach to *Monsanto*).

5. Identity Theft Is a Deprivation of Property and Other Rights Sufficient to Confer Standing

Home Depot argues that diminution in value does not confer standing because there is no ready market for personal and financial information. But this conclusion is directly contradicted by Plaintiffs' allegations that their information sold for between $50 and $100 on underground markets. Compl., ¶ 189. Home

[6] No. 14 C 1735, 2014 WL 4627893, at *3 (N.D. Ill. Sept. 16, 2014).

[7] No. 14-CV-4787, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014).

Depot's internal documents support this conclusion by characterizing Plaintiffs' personal information as an "asset" of the company. *Id*., ¶¶ 232-36. Several recent privacy cases have recognized that diminution of value of personal information is a valid measure of damages. *See*, *e.g*., *Svenson v. Google Inc*., No. 13–cv–04080, 2015 WL 1503429, at *5 (N.D. Cal. April 1, 2015) (holding that allegations of diminution in value of her personal information are sufficient to show damages for pleading purposes); *In re Facebook Privacy Litig*., 572 Fed. Appx. 494 (9th Cir. 2014) (reversing district court's rejection of diminution of value measure of damages in privacy case). And Plaintiffs need not allege they have or will attempt to sell their personal information in order for it to have value. *See Svenson*, at *5. Plaintiffs' allegations here are likewise sufficient to constitute injury. *See* Compl., ¶¶ 2, 98. Moreover, standing may be grounded upon the invasion of statutory or common law rights.[8] The violation-of-rights doctrine has been applied in recent privacy litigation. *See In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *17 (N.D. Cal. Sept. 26, 2013) ("[a]ll Plaintiffs need allege

[8] *See Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982) ("[a]s we have previously recognized, the actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.") (internal citations omitted)); *Hammer v. JP's Sw. Foods, L.L.C.,* 739 F. Supp. 2d 1155, 1162 (W.D. Mo. 2010) (Fair and Accurate Credit Transactions Act "has created a legally protected interest in being handed a receipt that omits certain of plaintiff's credit card information" sufficient to confer standing) *Katz v. Pershing, LLC*, 672 F.3d 64, 72 (1st Cir. 2012) ("invasion of a common-law right . . . can constitute an injury sufficient to create standing") (citations omitted).

is an invasion of statutory. . . rights to survive a motion to dismiss on standing grounds"). Plaintiffs have standing for this reason as well.

6. Plaintiffs Have Standing to Bring an Unjust Enrichment Claim

Plaintiffs allege that Home Depot was unjustly enriched by its failure to take measures to appropriately safeguard Plaintiffs' data. Plaintiffs would not have made purchases with a payment card (or, at all) had the company disclosed these failures. *See* Compl., ¶¶ 329, 331. Other courts agree that a failure to disclose is inequitable under these circumstances. *See, e.g., Target*, at *23 ("'would not have shopped' theory . . . is plausible and supports their claim for unjust enrichment."); *In re LinkedIn User Privacy Litig.*, No. 5-12-CV03088-EJD, 2014 WL 1323713, at *6 (N.D. Cal. March 28, 2014) (lax security practices might have affected consumers' behavior); *Adobe*, at *15-16 (same).

B. Plaintiffs' Injuries Are Fairly Traceable to the Breach

Because each Plaintiff alleges the harm flowing from the theft of their personal information was the direct result of Home Depot's conduct, Plaintiffs show traceability. *See* Compl., ¶¶ 4-11, 18-94. *See also Target*, at *2 ("Plaintiffs' allegations plausibly allege that they suffered injuries that are 'fairly traceable' to Target's conduct."); *Adobe*, at *10 (plausible allegations that injuries were 'fairly traceable' to failure to maintain reasonable security measures).

1. Criminality Does Not Immunize Retailers

Home Depot tries to sidestep liability altogether on the grounds that the breach was all the fault of the criminals who stole and sold Plaintiffs' information.

The Eleventh Circuit has rejected this reasoning because a "plausible inference" may arise that a defendant's "failures in securing [plaintiffs'] data resulted in their identities being stolen." *AvMed*, 693 F.3d. at 1330. This observation is consistent with other doctrines holding defendants liable for the foreseeable acts of independent third parties. *See Atlantic C. L. R. Co. v. Godard*, 211 Ga. 373, 377 (1955) ("The general rule that the intervening criminal act of a third person will insulate a defendant from liability for an original act of negligence does not apply when it is alleged that the defendant had reason to anticipate the criminal act.").

Home Depot also claims that it is "even more speculative" to suppose that criminals might partake in identity theft. Mtn. at 32. But as discussed above, this argument ignores the vast amount of information Home Depot maintained about each customer. *See* Compl., ¶¶ 230-31. Payment card data and personally-identifiable information allows identity thieves to fraudulently open new financial accounts, take out loans, incur charges, or clone payment cards. *Id*. ¶ 254. Further, customer location data allows criminals to circumvent traditional warning signs of identity theft. *See id*., ¶¶ 188, 256. Home Depot received warnings about potential security lapses exposing this trove of data, but ignored them. *See id*., ¶ 159. The limitations of foreseeability and causation do not protect the willfully ignorant.

C. Plaintiffs' Injuries are Redressable by a Favorable Ruling

Home Depot also contests the final element of Article III standing, redressability. At the pleading stage, courts typically find that plausible allegations of redressability are sufficient. *See*, *e.g.*, *AvMed*, 693 F.3d at 1324 ("Plaintiffs

allege a monetary injury and an award of compensatory damages would redress that injury. Plaintiffs have alleged sufficient facts to confer standing."); *Adobe*, at *10 (cost of mitigation and declaratory relief claims met standing requirements for redressability); *Target*, at *2, (standing met, and injuries could be redressed by injunctive relief).

Money damages, Home Depot suggests, are not available except to redress monetary harm. Putting aside what this rule would do to the constitutionality of the entire category of general damages, including pain and suffering, even Home Depot's cited authority acknowledges that money damages can redress the harm resulting from data breaches. *See SAIC*, 45 F. Supp. 3d at 33 (monetary reward could redress plaintiffs who suffered identity theft and invasion of privacy).

D. Plaintiffs Have Standing to Bring Claims in Jurisdictions Where There Is Not Yet a Named Plaintiff

Home Depot's argument that Plaintiffs must identify a class representative from each state is premature. Instead, it is sufficient at the pleading stage to allege that Home Depot operates in all 50 states and that individuals nationwide suffered injury. *See* Compl., ¶¶ 103-04, 190. Addressing this same argument in *Target*, the court held that "Article III standing analysis [for every state] is best left to after the class-certification stage." *Target*, at *4; *cf. Griffin v. Dugger*, 823 F.2d 1476, 1482 (11th Cir. 1987) (addressing issue at class certification). Indeed, consistent with Supreme Court precedent, the majority of courts hold this issue need not be resolved at the pleadings stage, as class certification is "logically antecedent" to

issues of Article III standing under state law. *Ortiz v. Fibreboard Corp*., 527 U.S. 815, 831 (1999); *see*, *e.g*., *Blessing v. Sirius XM Radio, Inc*., 756 F. Supp. 2d 445, 451 (S.D.N.Y. 2010) (referring to "growing consensus" that class certification is "logically antecedent [] where its outcome will affect the Article III standing determination"); *In re Hydroxycut Mktg. & Sales Practices Litig*., 801 F. Supp. 2d 993, 1005 (S.D. Cal. 2011) ("The constitutional issue of standing should not be conflated with Rule 23 class action requirements.").

Home Depot cites to *In re Flash Memory Antitrust Litig*., 643 F. Supp. 2d 1133 (N.D. Cal. 2009), but a data breach case is fundamentally different than an antitrust case, where "requirements of standing take on particular significance" because a balance must be struck between encouraging private actions and deterring legitimate activity through overly vigorous enforcement. *Target*, at *3; *City of Pittsburgh v. W. Penn Power Co*., 147 F.3d 256, 264 (3d Cir. 1998). Plaintiffs have alleged that Home Depot's conduct injured putative class members nationwide. *See* Compl. ¶¶ 103-04, 190, 196, 197, 206-07, 215, 218, 223. This is sufficient at the motion to dismiss stage: "To force Plaintiffs' attorneys to search out those individuals at this stage serves no useful purpose." *Target*, at *4.

II. Plaintiffs Adequately Allege Claims for Violations of State Consumer Protection Statutes

Plaintiffs have stated claims under the consumer protection statutes of 51 states and U.S. territories. *See* Compl., ¶ 290 (collectively, "consumer protection

statutes"). Plaintiffs have alleged facts showing that Home Depot violated the statutes based on several distinct fact patterns. These include Home Depot's:

> (1) Failure to maintain adequate computer systems and data security practices to safeguard Personal Information (*see* Compl., ¶¶ 119-75, 287-88);
>
> (2) Failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information (*see id*.);
>
> (3) Failure to timely and accurately disclose the data breach to Plaintiffs (*id*., ¶¶ 196-203, 222-23, 287-88);
>
> (4) Continued acceptance of card payments and storage of other personal information after exploitation of security vulnerabilities was known or should have been known (*id*., ¶¶ 119-175, 287-88); and
>
> (5) Continued acceptance of card payments and storage of other personal information after Home Depot knew or should have known of the breach and before it purportedly fixed the breach (*id*., ¶ 210, 287-88).

Plaintiffs have stated claims based on one or more of these theories for each consumer protection statute alleged in the Complaint. *See* Plaintiffs' Appendix 1 (setting forth violations of statutes and cross-referencing Plaintiffs' allegations).

A. Plaintiffs Suffered Actual Injury

Home Depot first contends that Plaintiffs have not alleged "actual injury" as required by the consumer protection statutes. *See* Mtn. at 40-41. But, as discussed above, Plaintiffs allege multiple categories of injury. *See* Compl., ¶¶ 261-62, 289. Most state courts construe consumer protection statutes liberally and interpret

injury limitations associated with those statutes broadly.[9] Plaintiffs' alleged injuries constitute "losses" as contemplated by these statutes. The *Target* court, addressing this exact issue, stated:

> Plaintiffs have pled economic injury, in the form of unreimbursed late fees, new card fees, and other charges. Regardless whether Plaintiffs have sufficiently pled economic injuries, however, the law is not as clear on this issue as Target argues. Although some states' statutes provide that a plaintiff may recover only for "ascertainable loss," that phrase is in general not limited to only purely economic loss, and includes other damages like loss of prospective customers[.]
>
> ***
>
> Plaintiffs have plausibly pled injury sufficient to meet the loss requirements in each of the jurisdictions from which their consumer protection claims stem. The determination whether all of the injuries Plaintiffs claim . . . are cognizable under each state's consumer-protection laws is a matter for summary judgment, not a motion to dismiss.

Target, at *5. The same conclusion is warranted here. The Court should also reject Home Depot's unsupported argument that injuries may have been caused by "plaintiffs themselves" or "independent third parties." Mtn. at 41. Assignment of fault is a question of fact. *See Smith v. Condry*, 42 U.S. 28, 31 (1843).

---

[9] *See, e.g., Craig & Bishop, Inc. v. Piles*, 247 S.W.3d 897, 907 (Ky. 2008) (ascertainable loss of money or property includes damages for future promises of financing, absences from work, inconvenience, and "constant telephoning"); *Serv. Rd. Corp. v. Quinn*, 698 A.2d 258, 264-65 (Conn. 1997) (loss of customers was ascertainable loss of money or property under unfair trade practices act that could support injunctive relief and attorneys' fees); *Weigel v. Ron Tonkin Chevrolet Co*., 690 P.2d 488, 494 (Or. 1984) (ascertainable loss of money or property should be "viewed broadly" and "may be so small that the common law likely would reject it as grounds for relief, yet it will support an action under the statute").

B. Plaintiffs Have Alleged Deceptive Acts and Practices

Home Depot next argues that Plaintiffs fail to allege facts demonstrating Home Depot's unfair or deceptive conduct and that this dooms their claims under the laws of 30 states. *See* Mtn. at 39, 41. But the categories of consumer protection violations discussed above constitute "deceptive" practices under the state laws. *See* Compl., ¶¶ 287-88. Acts and practices are deceptive, as here, when there:

> is a material representation, omission, act or practice that is likely to mislead consumers acting reasonably under the circumstances. A material representation, omission, act or practice involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product. An act or practice may be deceptive . . . regardless of a defendant's good faith or lack of intent to deceive.

In re Hannaford Bros. Co. Cust. Data Security Breach Litig., 613 F. Supp. 2d 108, 128-29 (D. Me. 2009) (interpreting Maine unfair practices statute, which is substantially similar to other states). The *Hannaford* court found that a delayed breach notification could be deceptive because:

> [a] jury could find that, if Hannaford had disclosed the security breach immediately upon learning of it from Visa, customers would not have purchased groceries at its stores with plastic during that period . . . until Hannaford contained the security breach . . . .

Id., at 129 (quotations and alterations omitted). Plaintiffs similarly allege that Home Depot knew its customer data was vulnerable to theft, but it did not warn customers of that fact. Compl., ¶¶ 119-31. After the breach, Home Depot failed to properly notify customers. Rather, it obscured the risks customers faced by claiming it was merely investigating "irregularities." *Id*., ¶¶ 185-86, 193, 198.

These types of omissions are "important to consumers" and "likely to affect their conduct." *Hannaford*, 613 F. Supp. 2d at 129. *See* Compl., ¶¶ 95, 222.

Moreover, contrary to Home Depot's suggestion, Plaintiffs' consumer protection claims are not fraud claims subject to the heightened pleading requirements under Rule 9(b). Courts from nearly every jurisdiction have held that allegations of deceptive acts or conduct under consumer protection laws are not subject to heightened pleading standards. *See*, *e.g.*, *Guerrero v. Target Corp*., 889 F. Supp. 2d 1348, 1355 (S.D. Fla. 2012) (consumer protection statute "enacted to provide remedies for conduct outside the reach of traditional common law torts like fraud," therefore "heightened pleading requirements of Rule 9(b) cannot serve as a basis to dismiss [Florida Deceptive and Unfair Trade Practices Act] claims.").[10] Home Depot cites no authority mandating heightened pleading and the Court should not impose such a requirement.

C. Plaintiffs Allege Facts to Support a Duty to Disclose

Home Depot claims 18 state laws do not recognize claims for material omission in the absence of a duty to disclose.[11] Yet Home Depot offers no

---

[10] *See also Garcia v. Crabtree Imports*, No. 3:05-CV-1324, 2006 WL 1646158, at *2 (D. Conn. June 14, 2006) ("Since fraud is not a necessary element of a state CUTPA claim . . . a plaintiff does not need to meet the heightened pleading requirements of Fed. R .Civ. P. 9(b)"); *Pelman ex rel. Pelman v. McDonald's Corp*., 396 F.3d 508, 511 (2d Cir. 2005) (refusing to apply heightened pleading requirements to New York General Business Law § 349).

[11] Home Depot's Appendix C, which it cites to support this argument, is not entirely accurate. *Contra* Appendix 2 hereto.

argument on the key issue: whether Plaintiffs' allegations give rise to a duty to disclose in states where it claims a duty is required.[12] A claim cannot be dismissed where a defendant fails to provide "any legal authority regarding the type of allegations that are sufficient to establish a duty to disclose under a state consumer-protection statute." *Target*, at *6. Although it is not Plaintiffs' burden to oppose an unsupported argument, Plaintiffs' Appendix 2 charts the duty in states where it is recognized and cross-references Plaintiffs' corresponding allegations.

Plaintiffs allege that Home Depot had a duty to disclose its security vulnerabilities, among other information, because it had exclusive knowledge that its inaction left customer data vulnerable to theft by hackers. Compl., ¶¶ 119-31. When the breach occurred, Home Depot had exclusive knowledge of the breach, the extent of the theft, and the time it took to secure its systems. *See id.* ¶¶ 185-86. That its security failings had been reported in the media does not erase a duty to disclose:

> It is one thing to have a poor reputation for security in general, but that does not mean that Adobe's specific security shortcomings were widely known. None of the press reports . . . discusses any specific security deficiencies, and Plaintiffs expressly allege that the extent of Adobe's security shortcomings were revealed only *after* the 2013 data breach.

[12] The one case it cites, *Infrasource, Inc. v. Hahn Yalena Corp.*, 272 Ga. App. 703, 704 (2005), does not apply. *Infrasource* did not involve a consumer fraud claim and, in any event, involved the law of Georgia, which is not one of the states whose consumer law is challenged by Home Depot. *See* Mtn. at App. C.

Adobe, 2014 WL 4379916, at *21; *see also* Compl., ¶ 211. To the extent a duty to disclose is a required element under any state's consumer protection law, Plaintiffs have alleged such a duty.

D. Plaintiffs Are Entitled to Injunctive Relief

Because they face a real and immediate threat of future injury, Plaintiffs have standing to seek injunctive relief under state consumer protection laws. The Complaint alleges that hackers intentionally targeted Plaintiffs' personal information, that Home Depot continues to store such personal information on its computer systems, that those systems remain insecure, and that hackers are aware that Home Depot is a vulnerable target. Another breach is inevitable unless the Court forces Home Depot to improve security. This attempt to prevent future harm is sufficient to establish standing. *See Sony*, 996 F. Supp. 2d at 999 (injunctive relief appropriate where plaintiffs "alleged that Sony's network security [was] still inadequate."); *Adobe*, at *13 (plaintiffs sufficiently alleged risk of future harm while seeking injunctive relief).

E. Plaintiffs Satisfy State-Specific Pleading Requirements

Home Depot's other arguments concerning state consumer protection claims cannot withstand scrutiny. *See* Mtn. at 43-46. First, Home Depot argues that neither the Delaware nor Oklahoma Uniform Deceptive Trade Practices Acts provide a private right of action. *See* Mtn. at 43. But Plaintiffs do not allege claims under those statutes. Instead, Plaintiffs allege violations of the Delaware Consumer Fraud Act and the Oklahoma Consumer Protection Act, both of which do provide a

private right of action. *See* Compl. ¶ 290.h, kk; Del. Code Ann. Title 6 § 2525(a); 15 Okl. Stat. Ann. § 761.1(A).

Second, Home Depot claims that the consumer fraud statutes of Alabama, Georgia, Kentucky, Louisiana, Mississippi, Montana, South Carolina, and Tennessee do not authorize class actions. *See* Mtn. at 44. The Supreme Court, however, has explained that Fed. R. Civ. P. 23 trumps conflicting state class action bars. *See Shady Grove Orthopedic Associates, P.A. v. Allstate Ins. Co.*, 559 U.S. 393 (2010). *Shady Grove* analyzed a New York statute that barred class actions. The plurality opinion explained that "[a] class action no less than traditional joinder . . . merely enables a federal court to adjudicate claims of multiple parties at once, instead of separate suits. And like traditional joinder it leaves the parties' legal rights and duties intact and the rules of decision unchanged." *Id*. at 408. Thus, class action prohibitions in state statutes, including the consumer protection statutes here, are merely procedural components that do not bar plaintiffs from bringing a class action in federal court. *See In re Hydroxycut Mktg. and Sales Practices Litig*., 299 F.R.D. 648, 651 (E.D. Mich. 2014) (permitting class actions under consumer protection statutes of Georgia, Louisiana, Montana, South Carolina, and Tennessee); *see also In re Lithium Ion Batteries Antitrust Litig.*, No. 13-MD-2420 YGR, 2014 WL 4955377, at *20 (N.D. Cal. Oct. 2, 2014).

The Eleventh Circuit, for instance, has applied *Shady Grove* in refusing to enforce a Georgia rule that conflicted with Rule 11 by mandating verified

complaints. *See Royalty Network, Inc. v. Harris*, 756 F.3d 1351, 1358 (11th Cir. 2014); *see also Palm Beach Golf Ctr.-Boca, Inc. v. John G. Sarris, D.D.S., P.A.*, 781 F.3d 1245, 1260 (11th Cir. 2015) ("The rules of procedure that apply in federal cases—even those in which the controlling substantive law is that of a state—are the Federal Rules of Civil Procedure.") (quotations omitted). Because class action procedure is governed by Rule 23, Plaintiffs can bring a class action in federal court under the consumer protection statutes of Alabama, Georgia, Louisiana, Mississippi, Montana, South Carolina, and Tennessee.

Third, Home Depot is incorrect that Kentucky prohibits class actions under its consumer fraud statute. *See* Mtn. at 44. The statute does not contain language barring class actions and both Kentucky district courts and the Sixth Circuit have affirmed the viability of class actions under the Kentucky Consumer Protection Act. *See* Ky. Stat. 367.110, *et seq.*; *Corder v. Ford Motor Co.*, 285 F. App'x 226, 229-30 (6th Cir. 2008) (vacating and remanding district court's dismissal of class action under the Kentucky Consumer Protection Act); *Naiser v. Unilever U.S., Inc.*, 975 F. Supp. 2d 727, 741 (W.D. Ky. 2013) (allowing class action under statute). Despite this authoritative case law, Home Depot cherry picks a District of Massachusetts opinion that addresses Kentucky law as part of a 50-state survey. *See In re Pharm. Indus. Average Wholesale Price Litig.*, 230 F.R.D. 61, 84 (D. Mass. 2005). This opinion is not authoritative.

Fourth, Home Depot contends that a class action under the consumer protection statutes of Ohio and Utah requires a declaration that an act is deceptive by a court's final judgment or by the state attorney general. *See* Mtn. at 44. As for Ohio, courts have held that the deceptive practices like those alleged in Count I are deceptive or unconscionable. *See*, *e.g.*, *Miner v. Jayco, Inc*., No. F-99-001, 1999 WL 651945, at *7-8 (Ohio Ct. App. Aug. 27, 1999). Moreover, the Utah Consumer Sales Practices Act should be liberally construed "to protect consumers from suppliers who commit deceptive and unconscionable sales practices." *Holmes v. Am. State Ins. Co.*, 1 P.3d 552, 557 (Utah App. 2000); *see also In re New Motor Vehicles Canadian Export Antitrust Litig.*, 350 F. Supp. 2d 160, 204 (D. Me. 2004) (denying motion to dismiss claim under the Utah Consumer Sales Practices Act). The Utah Consumer Sales Practices Act also "allows class treatment . . . when a consumer brings a claim for declaratory judgment [or] an injunction." *Miller v. Corinthian Colleges, Inc.*, 769 F. Supp. 2d 1336, 1342 (D. Utah 2011). The injunctive relief sought can sustain a class action on this claim. Compl., ¶ 292.

Finally, Home Depot claims that Plaintiffs cannot assert claims under the laws of 14 jurisdictions because no named Plaintiffs reside in any of these states. As explained *supra*, this argument is premature. Moreover, Home Depot misconstrues its cited authority, including *Mazza v. American Honda Motor Co*., 666 F.3d 581, 593 (9th Cir. 2012). There, the Ninth Circuit suggested that California consumer protection laws should not apply to residents of other states.

See Mtn. at 45-46 (also citing *In re Sony Gaming Networks and Customer Data Security Breach Litig.* ("*Sony I*"), 903 F. Supp. 2d 942, 964-65 (S.D. Cal. 2012), which relied on *Mazza*). Here, Plaintiffs do not seek to extend the reach of one state's consumer protection statutes to residents of other states—Plaintiffs seek to assert the statutory claims of each listed state on behalf of that state's residents.

III. Plaintiffs Have Adequately Pled Claims Under State Data Breach Laws

Plaintiffs allege claims under data breach notification statutes of 28 states. *See* Compl., ¶¶ 296-303. Home Depot does not challenge Plaintiffs' claims under five state statutes,[13] but it contends that 13 of the remaining statutes create no private right of action,[14] and that Plaintiffs have not alleged injuries under the remaining 10 statutes.[15] *See* Mtn. at 46-48, Apps. G, F. Home Depot also argues that the claims under the laws of nine states should be dismissed for lack of a named resident Plaintiff, *see* Mtn. at 46, n.18, App. H., an argument rebutted above. As set forth below, Plaintiffs state claims under these 28 state statutes.

A. Private Causes of Action May be Brought Under Challenged Statutes

Home Depot first challenges Plaintiffs' claims under statutes that do not expressly provide a private right of action. *See* Mtn. at 46. This overly restrictive reading is inconsistent with the underlying purpose of these statutes and relevant

---

[13] Alaska, Illinois, Maryland, New Jersey and North Carolina.

[14] Colorado, Delaware, Georgia, Iowa, Kansas, Kentucky, Michigan, Montana, North Dakota, Oregon, Puerto Rico, Wisconsin and Wyoming.

[15] California, District of Columbia, Hawaii, Louisiana, New Hampshire, South Carolina, Tennessee, Virgin Islands, Virginia, and Washington.

precedent. Of the 13 statutes challenged for no right of action, 10 use permissive language that implies a private right of action or permit enforcement through the states' consumer protection act. *See* Plaintiffs' Appendix 3. For example, the data breach statutes of Colorado, Delaware, Kansas, and Wyoming make clear that their enforcement provisions are "not exclusive" to the state attorney general. *See id*. Puerto Rico's data breach statute states, "the Secretary may impose fines . . . for each violation," but the "fines do not affect consumers' rights to initiate actions." *Id*. The laws of Iowa, Michigan, Montana, North Dakota, and Oregon invoke similar language. *See*, *e.g*., Iowa Code Ann. § 715C.2(9)(b) ("[t]he rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law."); *see also* Appendix 3. Under a plain reading of the statutes and in the absence of any authority stating no private right of action exists, Plaintiffs' claims may proceed. *See*, *e.g*., *Target*, at *13-14 (refusing to dismiss claims under data breach statutes with permissive language).

The statutes of Georgia, Kentucky, and Wisconsin are silent as to enforcement mechanisms,[16] but private enforcement furthers their underlying purpose. *See*, *e.g*., O.C.G.A. § 10-1-910(1), (4) (legislative findings by the Georgia assembly recognize need to "provide protection to consumers and the general public from identity thieves."). Kentucky has a sister statute that expressly permits private enforcement of any state statute. *See* Ky. Rev. Stat. § 446.070. The

[16] *See* O.C.G.A. § 10-1-912; Ky. Rev. Stat. Ann. § 365.732(2); Wis. Stat. §134.98.

Wisconsin law states that a violation of the data breach notification statute "may be evidence of negligence or a breach of a legal duty." Wis. Stat. Ann. § 134.98(4). Because Home Depot cites no authority that these states *forbid* private rights of action, the Court should not foreclose relief for residents of these states. *See Target*, at *13. Finally, Home Depot's reliance on *Pisciotta* is misplaced because that case only interpreted the Indiana data breach statute, whose *exclusive* remedies were "state enforced." *Pisciotta*, 499 F.3d at 637. Plaintiffs do not assert claims under Indiana's data breach statute.

B. Plaintiffs Allege Damages Flowing From Delayed Notification

Despite Home Depot's assertions to the contrary, Plaintiffs clearly alleged damages flowing from the delay in notification. First, Plaintiffs allege that:

> Despite having actual knowledge of the breach on September 2, 2014, Home Depot . . . [sat] idly by for six days as hackers openly sold at least 12 massive batches of Home Depot payment card data and customer information over the Internet. Because of Home Depot's delay in confirming it was the source of the breach, and delay in confirming the period of the data breach, financial institutions were reluctant to preemptively issue replacement cards to customers with Home Depot purchases, resulting in massive numbers of customers suffering fraud between September 2 and September 8, 2014.

Compl., ¶ 222. Had Home Depot confirmed the breach on September 2 (when it first possessed that knowledge), then many major financial institutions would have preemptively frozen customer accounts earlier. But by waiting until September 8, financial institutions were in limbo for six full days while massive quantities of cards were sold on underground markets and used to make fraudulent purchases.

Consumers who experienced fraud during this period suffered damages directly flowing from Home Depot's delay.

Moreover, Plaintiffs allege that Home Depot did not confirm that the malware had been cleared from its systems until September 18. Therefore, Home Depot "permitted its customers to keep using payments cards at its stores, and continue exposing their personal and financial data, for over two weeks after Home Depot had actual knowledge of the breach." *Id*., ¶ 210. Customers who shopped at Home Depot between September 2 and 18 represent another subset of individuals who suffered actual damages flowing from the tardy notification.

Finally, Plaintiffs allege that had Home Depot provided timely and accurate notice, Plaintiffs "could have avoided or mitigated the harm caused by the data breach." *Id.*, ¶ 301. These allegations are facially plausible and mitigation costs previously have been accepted as harms flowing from delayed data breach notification. *See Target*, at *15. Despite Home Depot's assertions, Plaintiffs explicitly allege multiple categories of damages flowing from Home Depot's delayed notification.

IV. Plaintiffs Have Adequately Pled Negligence Claims

Plaintiffs allege that Home Depot was negligent under Georgia law—or alternatively, under the laws of the individual states and U.S. Territories—by failing to protect personal and financial information and failing to provide proper notice of the breach. *See* Compl., ¶ 305; *John Crane, Inc. v. Jones*, 278 Ga. 747, 751 (2004) (reciting elements of negligence).

A. Plaintiffs Allege Home Depot Owed Its Customers a Duty and that Duty was Breached

> Plaintiffs allege Home Depot's breaches of the following duties:
>
> a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII and PCD in its possession;
>
> b. to protect [Plaintiffs'] PII and PCD using reasonable and adequate security procedures and systems that are compliant with the PCI-DSS standards and consistent with industry-standard practices; and
>
> c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying [Plaintiffs] of the Home Depot data breach.

Compl., ¶ 205. Home Depot claims that no duty exists because "general industry standards" do not create one. Further, it argues there is no common law duty to safeguard personal information or to provide notice of a data breach. Mtn. at 51. But Home Depot ignores the significant body of law recognizing that a "legal duty may arise from 'the general duty one owes to all the world not to subject them to an unreasonable risk of harm.'" *Underwood v. Select Tire, Inc*., 296 Ga. App. 805, 808-09 (2009) (quoting *Bradley Center v. Wessner*, 250 Ga. 199, 201 (1982)). Indeed, a duty arises when the risk of harm from one's conduct is "foreseeable" and "unreasonable." *Hodges v. Putzel Elec. Contractors*, 260 Ga. App. 590, 594 (2003).[17] Consistent with these principles, the Complaint alleges that "Home Depot owed a duty of care not to subject [Plaintiffs] to an unreasonable risk of harm

[17] *See also Coburn v. Lenox Homes, Inc*., 441 A.2d 620, 624 (Conn. 1982) ("A duty to use care may arise from a contract, from a statute, or from circumstances under which a reasonable person . . . would anticipate that harm of the general nature of that suffered was likely to result from his act or failure to act.").

because they were foreseeable and probable victims of any inadequate security practices." Compl., ¶ 306. Home Depot breached this duty by, among other things:

> a. creating a foreseeable risk of harm through the misconduct [described throughout the Complaint];
>
> b. failing to implement adequate security systems, protocols and practices sufficient to protect [Plaintiffs'] Personal Information both before and after learning of the data breach;
>
> c. failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the data breach; and
>
> d. failing to timely and accurately disclose that [Plaintiffs'] Personal Information had been improperly acquired or accessed.

Compl., ¶ 313. Other courts considering whether a duty is owed in similar situations agree. In *Sony*, for example, the court held that "the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity . . . [is] well supported by both common sense and [applicable state] law." *Sony II*, 996 F. Supp. 2d at 966; *see also AvMed, Inc*., 693 F.3d at 1326-28 (health care provider had duty to secure customers' information); *In re Zappos.com, Inc., Customer Data Security Breach Litig*., No. 3:12-cv-00325, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (finding duty "to protect Plaintiffs' private data from electronic theft with sufficient electronic safeguards"); *Claridge v. RockYou, Inc*., 785 F. Supp. 2d 855, 859, 866 (N.D. Cal. 2011) (recognizing duty where plaintiff application users directly provided their personal information to application developer); *Kahle v. Litton Loan Servicing LP*, 486 F. Supp. 2d 705, 708 (S.D.

Ohio 2007) ("[i]t is clear to the Court that Defendant owed a duty of care to [to protect customers' information] and that the duty was breached").

The authority cited by Home Depot is highly distinguishable because the plaintiffs had no direct relationship with the defendants. In *Willingham v. Global Payments, Inc.*, No. 1:12–CV–01157–RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013),[18] Magistrate Judge King recommended dismissing a negligence claim because the consumer plaintiffs sued a credit card processor—not a merchant—so there was "no direct relationship between the plaintiff and the defendant." *Id*. at *18. Judge King explicitly distinguished the facts of *Willingham* from *AVMed*, *RockYou*, and other cases where "the claimant had a direct relationship with the defendant and, therefore, had a basis for claiming that the defendant owed a duty of care." *Id*; *see also Target*, at *17 (noting the distinction).

Likewise in *Worix v. MedAssets, Inc*., 869 F. Supp. 2d 893 (N.D. Ill. 2012), the defendant was a "financial improvement partner for health care providers"—not a merchant—and had no direct relationship with the plaintiff. *See Worix*, 857 F. Supp. 2d 699, 700 (N.D. Ill. 2012) (earlier opinion discussing facts). In *Citizens Bank of Pa. v. Reimbursement Techs., Inc*., 2014 WL 2738220, at *3 (E.D. Pa. June 17, 2014), the court found that the parties' relationship was "a coincidence" and that the "unintentional nature of this connection weaken[ed] the inference of a relationship" sufficient to establish a duty. Unlike these cases, Home Depot had a

[18] *Willingham* has little persuasive value as the case was settled before the magistrate's recommendations were adopted or rejected by the district court.

direct relationship with its customers and used their personal and financial information for its own benefit. In so doing, Home Depot owed its customers a duty of care to protect their information and to provide fair notice of a breach. *Cf. Target*, at *14 ("Target does not dispute that Plaintiffs have plausibly alleged the existence of a duty."). To find otherwise would create a perverse result where retailers have carte blanche to use customer information for their own purposes without a corresponding obligation to protect it.

B. The Economic Loss Doctrine Does Not Bar Plaintiffs' Claims

The economic loss doctrine "generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort." *ASC Const. Equip. USA, Inc. v. City Commercial Real Estate, Inc*., 303 Ga. App. 309, 316 (2010) (quotations omitted). "The purpose of the economic loss rule is to distinguish between those actions cognizable in tort and those that may be brought only in contract." *Id*. This rule does not bar Plaintiffs' negligence claims.

First, the rationale underlying the rule is not satisfied where the parties have not expressly allocated risk through contract. *See Luigino's Int'l, Inc. v. Miller*, 311 F. App'x 289, 293 (11th Cir. 2009) (economic loss doctrine not applicable where "there is no contractual privity" between the parties).[19] Here, there is only an implied contractual relationship. Home Depot has cited to no Georgia case where

[19] *See also* O.C.G.A. § 51-1-11(a) ("no privity is necessary to support a tort action; but, if the tort results from the violation of a duty which is itself the consequence of a contract, the right of action is confined to the parties and those in privity to that contract[.]").

the economic loss rule was applied to preclude a negligence claim where the parties did not expressly allocate duties, obligations and risks through contract.[20]

Second, even if the rule could apply, several exceptions prevent its application here. The first is the "independent duty" exception: where "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." *Rosen v. Protective Life Ins. Co*., No. 1:09–CV–03620, 2010 WL 2014657, at *9 (N.D. Ga. May 20, 2010) (quotations omitted). "This principle has been applied in cases where the plaintiff identified a statutory or common law duty that would have existed absent the underlying contract." *Hanover Ins. Co. v. Hermosa Const. Grp*., LLC, 57 F. Supp. 3d 1389, 1396 (N.D. Ga. 2014) (citing *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)) (negligence claim not barred by economic loss doctrine where insurer had independent duty to act reasonably and in good faith). Here, Plaintiffs allege that Home Depot had "independent duties" to reasonably safeguard Plaintiffs' personal information and notify them of the breach. Compl., ¶ 312. These duties arise from both state and federal statutes, including Georgia's data breach notification law, Ga. Code Ann.

---

[20] *See Target*, at *19 (distinguishing *Sovereign Bank v. BJ's Wholesale Club, Inc*., 533 F.3d 162 (3d Cir. 2008), on which Home Depot relies, and noting "[b]ecause of the clear contractual relationship between the parties in *Sovereign Bank*, the application of the economic loss rule to bar the bank's negligence claim was more straightforward than application of the rule is in this case.").

§ 10-1-912(a), *et seq*. (creating legal duty for data collectors and information brokers to give notice of a data breach "in the most expedient time possible and without unreasonable delay"); and the Georgia Fair Business Practices Act, § 10-1-393(a), *et seq*. (creating legal duty for companies to refrain from engaging in "[u]nfair or deceptive acts or practices in the conduct of consumer transactions"). As discussed in *Hanover*, the economic loss rule does not apply where "the Georgia legislature created a cause of action independent of any underlying breach of contract claim." 57 F. Supp. 3d at 1397 (finding independent duty under Georgia's Uniform Fraudulent Transfers Act). Under federal law, the FTC Act, 15 U.S.C. § 45(a)(1), creates a legal duty for companies to refrain from engaging in "unfair or deceptive acts or practices in or affecting commerce." Courts have recognized that the FTC Act imposes a "reasonableness standard" and inadequate data security can constitute unfair practice under Section 5 of the Act. *See Wyndham*, 10 F. Supp. 3d at 616, 623 (agreeing with FTC that "in the data-security context, 'reasonableness is the touchstone' and . . . 'unreasonable data security practices are unfair'").

The second applicable exception is Georgia's "misrepresentation exception":

> One who supplies information during the course of his business, profession, employment, or in any transaction in which he has a pecuniary interest has a duty of reasonable care and competence to parties who rely upon the information in circumstances in which the maker was manifestly aware of the use to which the information was to be put and intended that it be so used. This liability is limited to a foreseeable person or limited class of persons for whom the information was intended, either directly or indirectly.

Holloman v. D.R. Horton, Inc., 241 Ga. App. 141, 148 (1999) (quotations omitted). The exception applies to situations of "passive concealment" as well as "constructive or actual" fraud. *Id*. at 797. Because Plaintiffs have alleged that Home Depot misrepresented and concealed material facts about its data security practices to customers (*see* Compl., ¶¶ 287-88), this exception also applies to preclude application of the economic loss doctrine.

Additionally, Georgia recognizes an "accident exception" to the economic loss doctrine: "[t]here is a general duty under tort law, independent of any contract, to avoid causing 'a sudden and calamitous event which . . . poses an unreasonable risk of injury to other persons or property.'" *Argonaut Midwest Ins. Co. v. McNeilus Truck & Mfg., Inc*., No. 1:11-CV-3495-TWT, 2013 WL 489141, at *4 (N.D. Ga. Feb. 8, 2013) (quotations omitted). Courts have applied this rationale to preclude application of the economic loss rule to a data breach fact pattern because it "present[s] a real danger of harm to persons or property":

> The data security breach is comparable to a tortious "accident" and the damages are of a type that caused economic harm to persons or entities. Indeed, tortious damages may include purely economic damages . . . [d]ismissal of the tort claims based on the economic loss rule is not appropriate.

Cumis Ins. Soc., Inc. v. Merrick Bank Corp., No. CIV07-374-TUC-CKJ, 2008 WL 4277877, at *8 (D. Ariz. Sept. 18, 2008). Likewise here, the accident exception applies because Home Depot's "sudden and calamitous" data breach posed an unreasonable risk of harm to Plaintiffs.

Finally, while Plaintiffs assert Georgia law applies to the nationwide negligence class, Plaintiffs additionally submit herewith Appendix 4, which rebuts Home Depot's contention that the economic loss doctrine bars Plaintiffs' negligence claims under the laws of 16 states. Undertaking a similar analysis in *Target*, that court concluded that the doctrine did not bar claims in the vast majority of states. *See Target*, at *15-20.[21]

C. Plaintiffs Have Alleged Injury

Plaintiffs do not allege that they were damaged merely because their personal information was "exposed." Rather, they allege non-speculative damages arising from the actual theft and misuse of their private information, as highlighted above. For the same reasons, Plaintiffs have alleged injury sufficient to satisfy standing under Article III, Plaintiffs satisfy the injury requirement for negligence.

V. Plaintiffs State a Claim for Breach of Implied Contract

Home Depot invited customers to use their credit or debit cards in order to increase sales by making purchases more convenient. *See* Compl. at ¶ 318. Implicit in this invitation was a promise to adequately safeguard Plaintiffs' personal information and to timely notify them of any breach. *See id*., ¶¶ 231, 317-19. Plaintiffs accepted Home Depot's offers by using their credit or debit cards to

[21] The *Target* court found only five states in which it believed the economic loss rule barred the negligence claims, *id.* at *19, but in some cases the plaintiffs failed to raise relevant exceptions. *See* Plaintiffs' Appendix 4.

make purchases. *See id*., ¶ 321. Home Depot breached its implied contracts and Plaintiffs suffered losses as a result. *See id*., ¶¶ 324-25.

Home Depot argues Plaintiffs have failed to allege a "shared intent" or "meeting of the minds" to enter into an implied contract for the protection of their Personal Information. *See* Mtn. at 53. Courts have consistently rejected this argument in data breach cases involving retail merchants, finding that "a determination of the terms of an alleged implied contract is a factual question that a jury must determine." *Target*, at * 21 (citing *Hannaford*, 613 F. Supp. 2d at 118-19 (D. Me. 2009)) (jury issue); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (same); *Irwin v. RBS Worldplay*, No. 1:09-cv-00033-CAP (N.D. Ga. Feb. 5, 2010) (Doc. 59) (allowing breach of implied contract claim in data breach case) (attached hereto as Exhibit E); *In re Michaels Stores Pin Pad Litig*., 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) (retail transaction created "an implicit contractual relationship between Plaintiffs and Michaels, which obligated Michaels to take reasonable measures to protect Plaintiff's financial information and notify Plaintiffs of a security breach within a reasonable amount of time."). As to Home Depot's contention that Plaintiffs have not alleged a cognizable injury, Plaintiffs refer the Court to their standing discussion above. s*upra*, Part I.

VI. Plaintiffs Have Adequately Pled a Claim for Unjust Enrichment

The elements of an unjust enrichment claim are that "(1) a benefit has been conferred, (2) compensation has not been given for receipt of the benefit, and (3) the failure to so compensate would be unjust." *Clark v. Aaron's Inc.*, 914 F. Supp.

2d 1301, 1309 (N.D. Ga. 2012). Plaintiffs conferred benefits on Home Depot when they purchased products and services. *See* Compl., ¶¶ 103, 327. However, Home Depot failed to invest a sufficient portion of those funds in projects and programs to protect their personal information, even though it knew about its security vulnerabilities for years before the breach. *See id*. ¶¶ 106, 119-20, 159, 327. Home Depot, therefore, has been unjustly enriched by retaining revenues from sales that should have been spent on data security. The Eleventh Circuit has recognized claims for unjust enrichment in similar circumstances. *See AvMed*, 693 F.3d at 1328 (allowing similar claim to survive a motion to dismiss).

Home Depot also was unjustly enriched because Plaintiffs would not have made purchases at Home Depot had they known of the security vulnerabilities. *See* Compl., ¶ 331. In *Target*, the court found plaintiffs' "would not have shopped" theory plausible to support a claim for unjust enrichment because "a reasonable jury could conclude that the money Plaintiffs spent at Target is money to which Target 'in equity and good conscience' should not have received." *Target*, at *23. The same ruling is warranted here.

VII. Plaintiffs' Declaratory Judgment Claim is Sufficiently Pleaded

Plaintiffs' declaratory judgment claim asks the Court to adequately secure Plaintiffs' personal information and declare whether Home Depot must implement additional security measures to fulfill its obligations. There are actual controversies regarding Home Depot's obligations and what security measures should be required. While Home Depot contends that its post-breach security measures are

adequate, *see* Compl., ¶ 340, Plaintiffs contend that the security flaws exploited during the data breach are just a few of the systemic vulnerabilities in its systems. *Id*., ¶¶ 338-40. Moreover, the widespread publication post-breach of Home Depot's lax attitude towards data security has made it an even more attractive target for hackers and increased the level of security that can be considered adequate or industry standard for Home Depot. *See id*., ¶¶ 133, 150-51, 158-61.

Plaintiffs request that the Court declare that Home Depot's common law duties and contractual obligations require it to implement several security measures that would have prevented or mitigated the data breach. *See id*., ¶ 341. These include: (1) conducting regular security audits and penetration tests to identify security vulnerabilities and fixing the vulnerabilities identified; (2) monitoring Home Depot's systems for security intrusions; (3) segmenting customer data using access controls and firewalls so that even if hackers gain access to one part of Home Depot's systems, they cannot access personal information; (4) deleting personal information that Home Depot no longer needs; and (5) ensuring that Home Depot's security personnel are adequately trained regarding Home Depot's security procedures and how to prevent, identify, and respond to data breaches.

A. Plaintiffs Have Standing to Seek a Declaratory Judgment

Home Depot contends that Plaintiffs lack standing and that they seek an impermissible advisory opinion. *See* Mtn. at 56-58. The Article III standing inquiry applicable to declaratory judgment claims asks whether the dispute is "definite and concrete, touching the legal relations of parties having adverse legal interests";

"real and substantial"; and amenable to "specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." *Medimmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007). Plaintiffs' declaratory judgment claim meets these requirements.

The dispute is definite and concrete as it concerns the parties' legal relations, including Home Depot's duty to protect Plaintiffs' personal information. *See* Compl., ¶¶ 304-25; Mtn. at 48-54. The parties are adverse in that Plaintiffs claim Home Depot's security measures remain insufficient, while Home Depot maintains that they are adequate. *See* Compl., ¶ 340. The dispute is real and substantial in that Home Depot has a history of ignoring security warnings, its security practices led to one of the largest data breaches in history, it still possesses Plaintiffs' personal information, and it remains vulnerable to attack. Finally, the dispute seeks conclusive relief that will determine whether and to what extent Home Depot must augment its security measures.

Home Depot refuses to acknowledge that the adequacy of its current security measures is even in dispute. Instead, it argues there is no real and immediate threat of future injury. *See* Mtn. at 57. Binding Eleventh Circuit precedent, however, establishes that Plaintiffs' allegations are sufficient. In *Strickland v. Alexander*, 772 F.3d 876 (11th Cir. 2014), the court held that a judgment debtor plaintiff had standing to bring a declaratory judgment action challenging the constitutionality of

Georgia's post-judgment garnishment statute even after the garnished funds had been returned to him. There, the plaintiff alleged that he remained a judgment debtor, had other debts, a very modest income, and funds in an account that likely were subject to garnishment under the statute. *Id.* at 885. Citing these facts, the court found standing because it was "simply a matter of time" before another creditor tried to garnish the plaintiff's funds. *Id.*

Home Depot ignores this precedent and instead relies on *Malowney v. Federal Collection Deposit Group*, 193 F.3d 1342 (11th Cir. 1999), an earlier case in which the plaintiffs challenged a similar Florida garnishment statute. *Id.* Unlike in *Strickland*, the *Malowney* plaintiffs did not allege that they were still judgment debtors or were likely to remain so for some time. *See Strickland*, 772 F.3d at 883-85 (distinguishing *Malowney* on this basis). Here, Plaintiffs' facts follow closer to *Strickland*: Home Depot still possesses Plaintiffs' personal information, *see* Compl., ¶¶ 231-32, 337; that information remains vulnerable to future attacks, *id.* ¶ 340; and hackers know that Home Depot remains an easy target, *id.* ¶ 339. Accordingly, Plaintiffs have standing to seek prospective declaratory relief.

B. Plaintiffs' Permissibly Seek A Declaration of Their Implied Contract Rights

Home Depot curtly contends that Plaintiffs cannot seek "a declaration that Home Depot has breached its contractual obligations" without alleging all of the elements of a breach of contract claim. Mtn. at 58. This argument mischaracterizes Plaintiffs' claim, which does not seek a decree that Home Depot *has breached* its

contractual obligations. Rather, Plaintiffs seek a declaration clarifying Home Depot's *ongoing* implied contractual obligations. In fact, in *Adobe*, the court rejected an identical argument[22] and declared that this is "precisely the type of relief that the Declaratory Judgment Act is supposed to provide." *Id.* at *14.

VIII. Plaintiffs State Claims Under California's Customer Records Act And Unfair Competition Law and Maryland's Personal Information Protection Act And Consumer Protection Act

Both the California Customer Records Act ("CRA"), Cal. Civ. Code § 1798.80 *et seq.*, and Maryland's Personal Information Protection Act ("MPIPA") Md. Code Ann., Com. Law § 14-3503, require businesses to "implement and maintain reasonable security procedures and practices" when storing individuals' personal information. Cal. Civ. Code § 1798.81.5(a)(1); Md. Code Ann., Com. Law § 14-3503.[23] Plaintiffs allege that Home Depot failed to implement "reasonable security measures" by (a) failing to identify, develop, and staff adequate data security measures between 2002 and 2010 (Compl., ¶¶ 106-18); (b) ignoring major security vulnerabilities in its management software, including in 2010-11 (*see id.*, ¶¶ 119-32); (c) failing to maintain appropriate software,

---

[22] *See Adobe*, at *14 (distinguishing the lone authority Home Depot cites in support, *Household Financial Servs., Inc. v. N. Trade Mort. Corp.*, No. 99-2840, 1999 WL 782072 (N.D. Ill. Sept. 27, 1999)).

[23] Both states also require timely notification of the data breach. *See* Md. Code Ann., Com. Law § 14-3504 (requiring companies to provide notice "as soon as reasonably practicable."); Cal. Civ. Code § 1798.82(a) (requiring notice "in the most expedient time possible and without unreasonable delay."). These provisions are included in the data breach notification claim.

monitoring, staffing, and procedures for data security in order to maximize profits (*see id*., ¶¶ 133-57); and (d) failing to update its security systems, including its point-of-sale device security, despite clear vulnerability warnings and actual malware intrusions in 2013 and 2014 (*see id*., ¶¶ 158-75).

Plaintiffs seek damages for Defendant's CRA violations under Cal. Civ. Code § 1798.84(b), which allows "[a]ny customer injured by a violation of this title" to "institute a civil action to recover damages." *Id.* (cited at Compl., ¶ 345). And Plaintiffs are entitled to injunctive relief under Cal. Civ. Code § 1798.84(e), which provides that "[a]ny business that violates . . . this title may be enjoined." Home Depot ignores this clear right to damages under Cal. Civ. Code § 1798.84(b) and cites inapposite cases that do not concern the CRA or data breaches.[24] Other courts have recognized that allegations similar to Plaintiffs' state a claim under the CRA and under California's Unfair Competition Law ("UCL"). *See Sony II*, 996 F. Supp. 2d at 1010 (denying motion to dismiss claim for injunctive relief under CRA); *Adobe*, at *17 (denying motion to dismiss CRA claim, based on alleged

[24] *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 466-67 (2013), concerned alleged violations of California's Shine the Light Law ("STL"), Cal. Civ. Code § 1798.83, which Plaintiffs do not invoke in this action. With regard to § 1798.84's damages and injunctive relief provisions, the *Boorstein* court merely recognized that a plaintiff must have "been 'injured by a violation of this title'" to pursue such remedies. *Id.* at 467 (quoting Cal. Civ. Code § 1798.84(b)). Defendant's citation to *Haskins v. Symantec Corp.*, 2013 WL 6234610 (N.D. Cal. Dec. 2, 2013) is similarly inapposite. That case did not concern the CRA or a data breach disclosing consumer data of any variety. Rather, that case concerned disclosure of antivirus software's source code.

failure to implement reasonable security measures and motion to dismiss claim under UCL's "unlawful prong").[25]

Likewise, the MPIPA states that a violation of that act constitutes a violation of Maryland's Consumer Protection Act ("MCPA"). Md. Code Ann., Com. Law § 14-3508. Under the MCPA, "[i]t is not necessary that a consumer actually have been misled or damaged as a result of the practice. The [MCPA] is to be construed liberally to promote the protection of consumers." *Scull v. Groover, Christie & Merritt*, *P.C.*, 76 A.3d 1186, 1193 (Md. 2013) (citations omitted). On behalf of Maryland Class members, Plaintiff Burden alleges actual injuries in the form of unauthorized charges and other injury. *See* Compl., ¶ 57. Such injuries are "objectively identifiable" and measurable losses, and thus cognizable under the MCPA. *See Lloyd v. General Motors Corp.*, 916 A.2d 257, 277 (Md. 2007).

CONCLUSION

Home Depot's Motion to Dismiss should be denied in its entirety. Alternatively, if this Court finds any of Plaintiffs' claims are subject to dismissal, Plaintiffs respectfully request leave to amend their Complaint.

---

[25] The *Adobe* court denied a motion to dismiss CRA and UCL claims analogous to Plaintiffs' claims in this case although Plaintiffs' claims here are even stronger given the allegations that many named Plaintiffs and class members have suffered identity theft and fraudulent charges on their cards as a direct result of the data breach at issue in this case. *See Adobe*, at *10. The *Adobe* court reasoned: "an injury that satisfies Article III's injury-in-fact standard suffices to establish statutory injury under the CRA." *Id*. at *11 (citations omitted).

Dated: July 1, 2015

Respectfully Submitted,

/s/ John R. Bevis

David J. Worley
James M. Evangelista
HARRIS PENN LOWRY, LLP
400 Colony Square
1201 Peachtree Street, NE, Suite 900
Atlanta, GA 30361
Telephone: 404-961-7650
Fax: 404-961-7651
david@hpllegal.com
jim@hpllegal.com

Consumer Co-Lead Counsel
and Steering Committee Members

Roy E. Barnes
John R. Bevis
THE BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Telephone: 770-227-6375
Fax: 770.227.6373
roy@barneslawgroup.com
bevis@barneslawgroup.com

Consumer Liaison Counsel
and Steering Committee Members

John A. Yanchunis, Sr.
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N Franklin Street
Tampa, FL 33602
Telephone: 813-223-5505
Fax: 813-223-5402
jyanchunis@forthepeople.com

Consumer Co-Lead Counsel
and Steering Committee Member

Norman E. Siegel
Barrett J. Vahle
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Telephone: 816-714-7100
Fax: 816-714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com

Consumer Co-Lead Counsel
and Steering Committee Members

Tina Wolfson
AHDOOT AND WOLFSON, P.C.
1016 Palm Avenue
West Hollywood, CA 90069
Telephone: 310-474-9111
Fax: 310-474-8585
twolfson@ahdootwolfson.com

Consumer Plaintiffs'
Steering Committee Member

Daniel C. Girard
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, CA 94108
Telephone: 415-981-4800
Fax: 415-981-4846
dcg@girardgibbs.com

Consumer Plaintiffs'
Steering Committee Member

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma, OK 73120
Telephone: 405-235-1560
Fax: 405-239-2112
wbf@federmanlaw.com

Consumer Plaintiffs'
Steering Committee Member

Gary S. Graifman
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
210 Summit Avenue
Montvale, NJ 07645
Telephone: 201-391-7600
Fax: 201-307-1086
ggraifman@kgglaw.com

Consumer Plaintiffs'
Steering Committee Member

Howard T. Longman
STULL STULL & BRODY
6 East 45th Street
New York, NY 10017
Telephone: 212-687-7230
Fax: 212-490-2022
hlongman@ssbny.com

Consumer Plaintiffs'
Steering Committee Member

CERTIFICATE OF SERVICE

I hereby certify that on this day I served the above and foregoing on all parties by causing a true and correct copy to be filed with the court's electronic filing system, which automatically sends a copy to all counsel of record.

/s/ John R. Bevis

John R. Bevis
Roy E. Barnes
THE BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060

Consumer Liaison Counsel and Steering Committee Members