UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Consumer Cases	MDL No. 14-2522 (PAM/JJK)

CONSUMER PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE

Cases

Statutes

Rules

I. INTRODUCTION

Rarely does a case in an evolving area of law create the opportunity to apply well-reasoned precedent, established principles and common sense to compelling facts showing widespread consumer harm and on issues of significant public importance. This is that case.

Between about November 15, 2013 and December 17, 2013, Target Corporation ("Target") was subject to one of the largest data breaches in history. Hackers stole the personal and financial information of up to 110 million Target customers. Consumer Plaintiffs ("Plaintiffs") are 112 of those customers – all injured as a direct result of Target ignoring its own warning systems that detected the breach, missing multiple opportunities to stop the breach, and unlawfully delaying informing customers after learning of the breach. Even after the Department of Justice ("DOJ") confirmed the breach, Target waited another seven days to tell the public – all the while continuing to accept customer debit and credit cards during the busiest part of the holiday shopping season.

Target's position is that because it was hacked by a third-party criminal, it has absolutely no legal duty or obligation to any Plaintiff – under any set of facts. But Target is not being sued simply because its systems were hacked. Target is being sued for its own misconduct – failing to take adequate and reasonable measures to safeguard its customers' data, failing to take available steps to prevent the breach from happening, failing to disclose that it lacked adequate computer security systems or protocols to safeguard customers' data, and failing to provide timely and adequate notice of the

breach after its own systems detected it, and for seven days after the DOJ confirmed the breach.

II. STATEMENT OF FACTS

The facts set forth in great detail in Plaintiffs' Complaint are critical to the disposition of Target's motion. Plaintiffs refer the Court to those allegations. Compl. ¶¶ 121-238.[1] Plaintiffs here provide capsule summaries of the following essential facts:

- Target failed to take numerous actions it could have taken, despite repeated warnings, to prevent the data breach from ever happening, including these examples. ¶¶ 122-170.

- Target failed to implement numerous security measures recommended by Visa to enhance security on the operating system Target employed. ¶¶ 127-130.

- Target failed to take any action after its computer systems alerted it to the breach as it was happening, including on November 30 and December 2, 2013. ¶¶ 152-157.

- Target turned off a malware security function that would have automatically deleted any malware detected before the breach. Had it not turned off this automatic security feature, the breach never would have occurred. ¶ 186.

- Target failed to segment its computer systems and require two-factor authentication for vendors. ¶¶ 147-150.

- Target could have prevented the breach by eliminating unneeded default accounts and requiring vendors to monitor their computer systems. ¶¶ 136-141, 155.

- Target could have prevented the breach by only allowing its network to upload to approved servers. ¶¶ 161-162.

[1] In this memorandum, citations to paragraphs in Plaintiffs' Consolidated Class Action Complaint (ECF No. 182) appear as "¶ __."

- Target failed to heed warnings by Visa, government agencies, researchers and members of its own security staff about the vulnerabilities in its systems. ¶¶ 126-131.

- A report by the United States Senate Committee on Commerce, Science and Transportation ("Senate Report") concluded that "Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach." ¶ 187. The report cited critical failures, including giving network access to a third-party vendor, failing to respond to automated warnings from its anti-intrusion software, failing to partition its sensitive network areas, and failing to respond to warnings from its anti-intrusion software regarding the escape routes the attackers would use to exfiltrate data. *Id.*

- Target's unlawful data retention practices exacerbated the breach. Target retains Plaintiffs' card data beyond the limits set by Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64, which prohibits retention of "card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in a case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction." This violation allowed the breach to occur. ¶¶ 195-197. As explained by a leading security expert, "[Target] is a breach that should've never happened . . . the fact that three-digit CVV security codes were compromised shows they were being stored." ¶ 191.

- An investigation by *Bloomberg Businessweek*, based on conversations with "10 former Target employees familiar with the company's data security operation, as well as eight people with specific knowledge of the hack and its aftermath," found that the FireEye malware detection program used by Target worked but Target "stood by as 40 million credit card numbers – and 70 million addresses, phone numbers, and other pieces of personal information – gushed out of its mainframes." ¶ 186. *Bloomberg* further reported:

> In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened. . . . Had the company's security team responded when it was supposed to, the theft that has since engulfed Target, touched as many as one in three American consumers, and led to an international manhunt for the hackers never would have happened at all.
>
> As the hackers inserted more versions of the same malware (they may have used as many as five, security researchers say), the

> security system sent out more alerts, each the most urgent on FireEye's graded scale, says the person who has consulted on Target's probe.
>
> The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it's detected. But according to two people who audited FireEye's performance after the breach, Target's security team turned that function off. *Id.*

- The data stolen in the breach quickly flooded the black market, where it has been further misused through sales on illegal card shop websites at prices of up to $135 per card. ¶¶ 164-167.

- As numerous governmental and other reports have concluded, consumers' personal and financial information stolen from Target is extremely valuable to thieves. ¶¶ 213-226.

- Target failed to disclose the highly material facts that its computer systems and security practices were inadequate and to provide timely and accurate notice of the breach. ¶¶ 228-229. Had Target disclosed its inadequate security practices, Plaintiffs would not have made purchases using their credit or debit cards and would not have purchased goods at all from Target during the breach. ¶ 231. Target continued to accept payment cards after it knew or should have known that its systems had been breached and without disclosing the breach in a timely manner. ¶ 252.

- Target failed to meet its obligations under state data breach notice statutes by unreasonably delaying telling the public about the breach. Target did not disclose the breach on November 30, 2013 or December 2, 2013, when its own security systems alerted it to the hackers' malware; nor from December 2-15, when the hackers collected customers' data and sent it to three staging points within Target's computers where it sat for six days before the hackers sent the data offshore; nor on December 11, when a Target employee detected the malware and sent it outside Target for evaluation; nor on December 12, after DOJ alerted Target to the breach; nor on December 15, when Target started purging the hackers' malware from its system. ¶¶ 270-282.

- Only after news of the breach broke in the media – and seven days after DOJ told Target of the breach – did Target tell the public. ¶¶ 171-174, 279.

- Target's misconduct has injured consumers nationwide. ¶¶ 1-119.

These egregious facts, set forth in far greater detail in Plaintiffs' Complaint, distinguish this case from other data breach cases. They compel denial of Target's motion. The rest of this brief provides the legal authorities and analysis, leading to the same ineluctable result.

III. LEGAL STANDARD

"Defendant carries a heavy burden in seeking dismissal pursuant to Fed. R. Civ. P. 12(b)(6)." *Grillo v. John Alden Life Ins. Co.*, 939 F. Supp. 685, 687 (D. Minn. 1996). In considering a motion to dismiss under Rule 12(b)(6), "the Court takes all facts alleged in the complaint as true." *Mack v. Stryker Corp.*, No. 10-2993 (PAM/JJG), 2010 WL 4386898, at *1 (D. Minn. Oct. 28, 2010) (citation omitted). "The Court must construe the factual allegations in the complaint and reasonable inferences arising from the complaint favorably to the plaintiff . . . ." *Id.* (citation omitted). A complaint must include "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 569 (2007). A claim is plausible when plaintiff "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "*Twombly* and *Iqbal* did not abrogate the pleading standard of Rule 8(a)(2)." *Mack*, 2010 WL 4386898, at *1 (citing *Hamilton v. Palm*, 621 F.3d 816, 817 (8th Cir. 2010)). A defendant "cannot rely on the facts as it sees them to establish its entitlement to a dismissal" because the Court "takes the facts as pled and determines whether those facts plausibly support a cause of action." *HomeStar Property Solutions, LLC v. Statebridge Co.*, No. 13-1240 (PAM/SER), 2013 WL 5787667, at *4 (D. Minn. Oct. 28, 2013) (noting that defendant's

disagreement with plaintiff "is not something the Court can consider on a Motion to Dismiss"). Further, "the complaint should be read as a whole, not parsed piece by piece to determine whether each allegation, in isolation, is plausible." *Braden v. Wal-Mart Stores, Inc.*, 588 F.3d 585, 594 (8th Cir. 2009).

IV. PLAINTIFFS HAVE ARTICLE III STANDING.

A. All Plaintiffs Satisfy Standing Requirements.

The long-settled Article III standing requirements are injury, fairly traceable to the defendant's conduct, and redressable by a favorable ruling. *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1147 (2013); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *Steger v. Franco, Inc.*, 228 F.3d 889, 892 (8th Cir. 2000). The allegations of the Complaint satisfy all three requirements, as the following examples illustrate.

The debit card of Plaintiff Brystal Keller was compromised when she used it to make purchases at a Target store in Missouri during the breach. She was unable to withdraw her own money from an ATM because her card was declined. Ms. Keller had two fraudulent charges on her account from unauthorized purchases on December 26, 2013: one for $434.15 at a Target store in New York and another for $276.00 from a purchase made in South Carolina. Ms. Keller's bank did not reimburse either fraudulent charge until January 7, 2014, more than two weeks after the fraud occurred. Ms. Keller was locked out of her account from December 26 until January 21. As a result, she missed a rent payment, a car loan payment and a washer and dryer payment, resulting in unreimbursed fees of $150, $34 and $15, and had trouble putting food on the table for her family during the holidays. ¶ 1.a.

Plaintiff Aimee King had seven unauthorized charges on her bank account totaling approximately $140 after using her debit card to shop at a Target store in California during the breach. Ms. King was the sole income earner for her family. As a result of the unauthorized charges, she was unable to pay bills, including car insurance, rent, loan and cell phone bills. She incurred about $275 in unreimbursed late fees and had to borrow money from her mother to cover the rent. The interest rate on her loan increased from 50% to 175% and her credit score dropped by about 40 points, interfering with her plan to purchase a car. ¶ 1.b.

Plaintiff Christie Oliver used her debit card to purchase goods at a Target store in Texas during the breach. Her card was declined on December 22, when she discovered unauthorized charges on her account totaling $1,506.98. Her bank account was partially frozen, allowing her to access only $700 of her account funds until December 31. She had no money to complete her Christmas and grocery shopping. She was unable to host Christmas dinner, to visit or buy presents for her grandchildren, or to pay her mortgage payment on time, resulting in an unreimbursed late fee. She also had to pay unreimbursed replacement check fees. ¶ 1.c.

Plaintiff Deborah Rhodes used her debit card to make purchases at Target during the breach. She incurred an unauthorized charge of $3,900, resulting in a negative balance of $3,600 in the bank account held jointly with her husband. Ms. Rhodes receives disability payments and is paid via direct deposit. The account was frozen by the bank, resulting in missed bill payments and late fees. Ms. Rhodes and her husband had to file a police report and were forced to borrow money for two weeks to meet daily living needs.

Additionally, she purchased credit monitoring services for $70 per month. She has not been reimbursed for card replacement fees or late fees. ¶ 1.d.

When Plaintiff Michelle Mannion tried to purchase goods at a Target in Ohio during the breach, she discovered four unauthorized charges on her account totaling about $222. Her account was frozen. As a result, her plans to celebrate her daughter's 21st birthday on December 22 were spoiled and her holiday ruined. She lacked access to her account and worried about how to feed her children until her next paycheck. She broke down in tears after learning that her account was drained. ¶ 1.e.

Plaintiff Frederick Smart used his Target REDcard to purchase goods at a Target in Texas during the breach. He incurred fraudulent charges on his cards of approximately $378 in November and December. Following the breach, scammers opened multiple phony accounts in his name and attempted to open many others. He lost access to his funds and had restrictions placed on his account. After approximately 35 fraudulent inquires on his credit bureau records, his credit score dropped approximately 25-50 points, requiring him to delay purchasing a new car. He has received numerous scam telephone calls and mail, purchased credit monitoring services, incurred late payment fees and paid a replacement card fee. ¶ 1.f.

After Plaintiff Martha Reynoso used her EPPICard debit card at an Illinois Target store during the breach, her account was almost entirely drained. (The EPPICard is used by the state of Illinois to facilitate payment of child support.) On December 28, the balance in her account was depleted from $3,643.53 to $5.86 as a result of five unauthorized international ATM transactions. The large unauthorized withdrawals were

grossly at odds with Ms. Reynoso's use of her EPPICard for much smaller purchases in Illinois to pay living expenses for her son. As a result, her account was frozen from December 28 until January 14, leaving her no funds to care for her son. She was forced to borrow money and deplete some of her savings to feed her son and cover his tuition payments and to cut back on spending to make ends meet. She obtained a replacement EPPICard at an unreimbursed cost of $5.00. The unauthorized withdrawals were eventually reimbursed by her bank. ¶ 1.f.

Plaintiff Barbara Donald used her prepaid card to purchase goods at a Target store in Mississippi during the breach, causing her personal information to be compromised. She incurred multiple unauthorized charges to her account in December, lost access to her funds, incurred unreimbursed late fees for missed payments, and had household utilities shut off. She was unable to pay her mortgage, had to refinance her home loan and was compelled to borrow money to cover living expenses. ¶ 63.

These are only examples. Each Plaintiff describes the harm suffered as a result of the breach. ¶¶ 1-119. All Plaintiffs would not have used their credit or debit cards to make purchases at Target, and would not have shopped at Target at all during the breach, had Target told them that it lacked adequate computer systems and data security practices to safeguard customers' personal and financial information, and had Target provided them with timely and accurate notice of the breach. ¶¶ 1.g., 113.

Each Plaintiff suffered actual injury as a result of the Target data breach by paying money to purchase products from Target that they would not have made had Target properly disclosed its inadequate security safeguards and the breach. ¶¶ 114-115. All

Plaintiffs further allege actual injury in the form of diminution in the value of the personal and financial information they entrusted to Target. ¶ 116. All Plaintiffs allege that they were overcharged for purchases using their payment card during the breach in that a portion of the purchase price was for reasonable and adequate security which Target failed to provide. ¶ 117. Further, all Plaintiffs suffered imminent, certainly impending injury arising from the substantially increased risk of future fraud, identity theft and misuse now that their personal information is in the hands of criminals who sold it on the black market. ¶ 118.

Target's position that Plaintiffs lack standing ignores these facts and settled law.

1. All Plaintiffs Have Been Injured by Target's Unlawful Conduct.

The injury component of Article III standing may be satisfied by allegations of *either* "actual *or* imminent" injury. *Clapper*, 133 S. Ct. at 1147 (emphasis added). Plaintiffs suffered both.

As illustrated above, Plaintiffs suffered actual injury in multiple forms, including (1) theft of their credit or debit account and personal information (¶¶ 112, 114); (2) diminution in value of the information they entrusted to Target (¶ 116); (3) unauthorized charges on their payment card accounts, including unreimbursed charges and fees; (4) loss of access to funds in their accounts, forcing them to incur late payment fees, borrow money to meet living needs, and suffer harm to their credit; (5) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts, including purchasing credit monitoring services; and (6) overcharges for purchases because Plaintiffs did not receive the data security they paid for. ¶ 117.

2. All Plaintiffs Suffered Imminent and Certainly Impending Harm.

Although not required to establish standing, Plaintiffs have also alleged and factually supported imminent, certainly impending, injury arising from the substantially increased risk of future potential fraud, identity theft and misuse by criminals who have already sold Plaintiffs' personal and financial information on the internet black market. ¶ 118.

Courts have recognized standing even where no actual misuse has occurred, as it has in this case. *See, e.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007) (holding that "the 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) (holding that plaintiffs "whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III").

The Supreme Court's decision in *Clapper v. Amnesty Int'l USA* supports Plaintiffs' standing. There, the Court stated that "we have repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact.'" 133 S. Ct. at 1147 (citation omitted). The Court's application of this principle in *Clapper* rested on distinguishable facts. The plaintiffs, including attorneys and human rights and media organizations, sought a declaratory judgment that provisions of a federal statute allowing surveillance of certain individuals were unconstitutional. *Id.* at 1142. The Court denied standing because the threatened injury was not certainly impending where the plaintiffs

had "fail[ed] to offer any evidence that their communications have been monitored." *Id.* at 1148.

This case, by contrast, does not involve speculation about the occurrence of some future event. Plaintiffs have already incurred actual financial losses caused by a data breach that has already occurred and face a real, concrete and "certainly impending" threat arising from the sale of their personal information on the black market.

In *In re Sony Gaming Networks and Customer Data Breach Security Litigation*, the court rejected the defendant's argument that *Clapper* required dismissal on standing grounds, stating that "the Supreme Court's decision in *Clapper* did not set forth a new Article III framework" but "simply reiterated an already well-established framework for assessing whether a plaintiff had sufficiently alleged an 'injury-in-fact' for purposes of establishing Article III standing." 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014). The court found that "Plaintiffs' allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [is] sufficient to establish Article III standing at this stage in the proceedings." *Id.* at 962.

On facts similar to those before the Court, the district court in *In re Adobe Systems, Inc. Privacy Litigation*, No. 13-CV-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014), recently upheld the plaintiffs' standing in a data breach case. 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. *Id.* at *2. The court found that "the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*" because "the risk that Plaintiffs' personal data will be

misused by the hackers . . . is immediate and very real." *Id.* at *8. The court reasoned that "in contrast to *Clapper*, . . . there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken" or "whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so." *Id*. There, as here, "stolen data had already surfaced on the internet." *Id.* For that reason, "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) (holding that "the elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing").

3. Plaintiffs Allege Facts Showing Their Injuries Are Fairly Traceable to the Target Data Breach.

Plaintiffs also satisfy the standing requirement that their injuries be fairly traceable to the challenged conduct. Each Plaintiff alleges the harm flowing from compromise and theft of their personal information was the direct result of Target's conduct. ¶¶ 7-119. *See Adobe*, 2014 WL 4379916, at *10 (finding that plaintiffs plausibly allege that their injuries are 'fairly traceable' to Adobe's alleged failure to maintain reasonable security measures).

Target incorrectly maintains that Plaintiffs must allege purchases after November 30, 2013 when the hackers began stealing their information. Target cites no authority to

support this proposition and ignores the facts. Plaintiffs allege in detail that the breach was a dynamic process involving seven steps spanning three time periods. ¶¶ 123-193. Target arbitrarily focuses on November 15, the start of the third stage, when the hackers installed their data-stealing malware and began to collect cards from customer transactions. ¶ 151. The next two links in the kill chain (occurring from December 2-17) were also an essential part of the continuing course of conduct constituting the breach. During that time, the hackers collected customers' information, stored it on Target's own computer network for six days, laundered it through sham computer servers, and eventually sent it to the hackers' server in Russia—a process that continued unfazed for another two weeks. ¶¶ 158-160. Target's arbitrary selection of a single mid-stream date ignores the continuing, integrated nature of the breach.

Furthermore, Target admits that of the 110 million customers affected by the breach, the 70 million customers whose personal information was stolen included customers whose personal information was acquired by Target other than through card purchases during the breach. ¶¶ 179-180. That admission undermines Target's argument that only post-November 30 purchases matter.

Target also makes the puzzling assertion that Plaintiffs fail to specify what information of theirs was stolen. Plaintiffs do exactly that with detailed allegations, some invoking Target's own public disclosures, such as its December 19 announcement that "customer name, credit and debit card number, and the card's expiration date and CVV" of approximately 40 million customers was stolen (¶ 174); its December 27 announcement that "PIN data was removed" during the breach (¶ 178); and its January 10

announcement that the names, mailing addresses, phone numbers and email addresses of an additional 70 million customers were also stolen in the breach (¶ 179).

4. Plaintiffs' Injuries are Redressable by a Favorable Ruling.

Target does not contest that Plaintiffs satisfy the third component of Article III standing. Their injuries are clearly redressable by a judgment or court-approved settlement providing compensation and appropriate injunctive relief. *See Adobe*, 2014 WL 4379916, at *10 (finding that "the relief sought would redress these injuries").

B. Plaintiffs' Standing Is Further Supported by the Invasion of Their Legal Rights.

Supreme Court precedent and federal court decisions recognizing standing based on the invasion of legal rights further support Plaintiffs' standing. *See Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982) (stating, "[a]s we have previously recognized, '[t]he actual or threatened injury required by Art. III may exist solely by virtue of "statutes creating legal rights, the invasion of which creates standing . . . ."'" (quoting *Warth v. Seldin*, 422 U.S. 490, 500 (1975)) (additional citations omitted)); *Hammer v. JP's Sw. Foods, L.L.C.*, 739 F. Supp. 2d 1155, 1162 (W.D. Mo. 2010) (holding 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" and that "[v]iolation of that legally protected interest is a sufficient injury-in-fact to confer standing"). This standing 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) (holding that plaintiffs' allegations that defendant violated

California's anti-wiretapping and anti-eavesdropping statute established standing, and concluding that "[a]ll Plaintiffs need allege is an invasion of statutory . . . rights to survive a motion to dismiss on standing grounds").

This principle applies to common law rights. *See Katz v. Pershing, LLC*, 672 F.3d 64, 72 (1st Cir. 2012) (noting that "[t]he invasion of a common-law right (including a right conferred by contract) can constitute an injury sufficient to create standing") (citing *Ala. Power Co. v. Ickes*, 302 U.S. 464, 479 (1938)).

Target's alleged violations of rights conferred by statute (consumer protection statutes and state data breach statutes) or protected by common law causes of action (negligence, breach of implied contract, breach of Target's REDcard contract and unjust enrichment), as discussed below, are amply pled, further supporting Plaintiffs' standing.

C. Target's Challenges to Plaintiffs' Allegations of Imminent Injury Are Unavailing.

Target cites a number of cases in which courts have found plaintiffs lacked standing in data breach cases. All are inapposite or readily distinguishable.

In *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, No. 12-347, 2014 WL 1858458 (D.D.C. May 9, 2014), 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. *Id*. at *1. The court reasoned that the thief would not be able to misuse the data without an attenuated chain of events (including the thief recognizing the tapes for what they were and obtaining the specialized software needed to read the data) and could have simply sold the other

property and discarded the data tapes. *Id.* at *6. By contrast, the Target hackers breached its system for the purpose of stealing data that has been stolen and misused. *See Adobe*, 2014 WL 4379916, at *9 (distinguishing *SAIC*, noting that the "hackers targeted Adobe's servers in order to steal customer data" and that "some of the information stolen in the 2013 data breach has already surfaced on websites used by hackers").

In *In re Barnes & Noble Pinpad Litigation*, No. 12-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013), it was not clear that the plaintiffs' information had been taken. *See Adobe*, at *9 (distinguishing *Barnes & Noble* on those grounds). Similarly, in *Remijas v. Neiman Marcus Group, LLC*, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014), the district court distinguished the Seventh Circuit's opinion in *Pisciotta*, noting that "the plaintiffs here do not allege that data belonging to all of the customers at issue were in fact stolen" and that "the overwhelming majority of the plaintiffs allege only that their data *may* have been stolen." *Id.* at *3. Plaintiffs, by contrast, allege that their data was stolen

In *U.S. Hotel and Resort Management v. Onity, Inc.*, No. 13-1499 (SRN/FLN), 2014 WL 3748639 (D. Minn. July 30, 2014), the plaintiffs alleged that hotel locks could be easily opened by thieves, but did not allege that any locks had been breached. *Id.* at *3. Summarizing the relevant case law, the court noted that where plaintiffs have been

denied standing, they "have not yet had their identity stolen or their data otherwise actually abused." *Id.* at *5.[2]

Target also contends that Plaintiffs' allegations of imminent injury are merely legal conclusions. Plaintiffs' allegations are no such thing. As discussed above, they set forth specific facts that satisfy the standing requirements.

Target again misses the mark by criticizing Plaintiffs for not alleging "how likely plaintiffs are to become fraud victims." Def.'s Mem. at 9. Plaintiffs are not required to quantify the likelihood of harm. They have already been harmed, which distinguishes this case from *Galaria v. Nationwide Mutual Insurance Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014), in which the plaintiffs alleged only that consumers receiving a data breach notification have a fraud incidence rate of 19% in 2011. *Id*. at 654. *See Adobe*, 2014 WL 4379916, at *9 (finding "[*Galaria's*] reasoning unpersuasive – after all, why would hackers target and steal personal customer data if not to misuse it? – and declines to

[2] Other cases cited by Target are as readily distinguishable. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) (denying standing where "no evidence suggests that the data has been – or will ever be – misused"); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307, at *2, *7-8 (S.D.N.Y. June 25, 2010) (no evidence the information had been accessed or used inappropriately); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052 (E.D. Mo. 2009) ("plaintiff does not claim that his personal information has in fact been stolen"); *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *6-7 (N.D. Ga. Feb. 5, 2013) (suggesting plaintiffs' particular allegations, under different facts, were insufficient to show actual injury or imminent risk of future identity theft).

follow it" and that "*Galaria's* reasoning lacks force here, where Plaintiffs allege that some of the stolen data has already been misused").[3]

Also flawed is Target's contention that replacement cards, obtained by some Plaintiffs, eliminated any threat of harm. It ignores the multiple harms Plaintiffs have actually suffered, and that stolen data may be held for more than a year before being used to commit identify theft, and that fraudulent use of stolen data may continue for years. ¶ 182.[4]

D. Target's Arguments Challenging Plaintiffs' Allegations of Actual Injuries Fail.

Target also erroneously argues that various categories of actual injuries detailed in the Complaint do not establish standing.

---

[3] Target wrongly suggests that an offer of one year of free credit monitoring eliminates the risk of future injury. Plaintiffs allege that Target's limited offer of free credit monitoring is inadequate, that credit monitoring does nothing to prevent payment card fraud but only informs a consumer of instances of fraudulently opened accounts, not fraudulent use of existing cards. ¶ 182.

[4] Target shuts its eyes to the multiple injuries and overlapping bases for standing alleged by the very Plaintiffs it singles out. *See* Plaintiff Rhodes, ¶ 1.d. (unauthorized charges, lost access to account funds resulting in missed bill payments and late fees, filed police report, borrowed money to meet living needs, purchased credit monitoring and incurred unreimbursed card replacement fees and late fees); Smart, ¶ 1.f. (fraudulent charges, scammer opening multiple accounts, loss of access to account funds, adverse impact on credit score forcing delay in car purchase, scam mail and phone calls and credit monitoring costs); Reynoso, ¶ 1.g. (unauthorized charges drained account used for child support, compelled to borrow money, depleted part of savings and incurred unreimbursed cost of replacement card); Liston, ¶ 37 (unreimbursed replacement card fees and late payment fees); Fazio, ¶ 77 (unreimbursed replacement card fee and overdraft fee); Guercio, ¶ 82 (financial and personal information compromised); and Jefferson, ¶ 85 (unauthorized charges, unreimbursed replacement card fee, loss of access to funds).

1. Mitigation Costs.

Target misreads *Clapper* as a blanket holding that mitigation costs, including credit monitoring, cannot support standing.[5] But, as discussed, the plaintiffs in *Clapper* failed to establish that the surveillance they feared had occurred or ever would. Each of the other cases Target relies upon (*Remijas*, *Galaria* and *Barnes & Noble*) has already been distinguished.

In cases paralleling the facts before this Court, courts have recognized that mitigation costs may be recovered in data breach cases. *See, e.g.*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164 (1st Cir. 2011) (finding that mitigation costs supported standing for plaintiffs whose payment card information was stolen and used by sophisticated criminals, resulting in unauthorized charges and exposing all card users during the breach to the risk of unauthorized charges); *Adobe*, 2014 WL 4379916, at *9 (stating that mitigation costs incurred by consumers facing certainly impending future harm constituted an injury-in-fact).

2. Unauthorized Charges and Fees, and Loss of Access to Plaintiffs' Own Funds.

All Plaintiffs who allege unauthorized charges to their accounts and associated fees have standing. Courts have uniformly held that incurring unauthorized charges

[5] Target makes this argument in challenging Plaintiffs' showing of imminent injury. However, a number of Plaintiffs have already incurred mitigation costs, including purchases of credit monitoring services. *See* Plaintiffs Rhodes, ¶ 1.d.; Smart, ¶ 1.f.; Herring, ¶ 10; Dorobiala, ¶ 18; Boasso, ¶ 19; Eshtiyag, ¶ 21; Bok, ¶ 26; Lovelace, ¶ 68; Bryant, ¶ 69; Marciniak, ¶ 72; Boykin, ¶ 74; Noe, ¶ 87; and Nagro, ¶ 106.

confers standing. *See, e.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 133 (D. Me. 2009), *aff'd in part and reversed in part on other grounds*, 659 F.3d 151(1st Cir. 2011). The same is true of Plaintiffs who incurred unreimbursed fees.

Target's argument that Plaintiffs Melnichuk and Quillian failed to allege that their unreimbursed charges were "fairly traceable" to the breach fails because they, like all other Plaintiffs, allege that their losses directly resulted from the breach [6]

Also unavailing is Target's argument that Plaintiffs who did not allege that unauthorized charges were not reimbursed lack standing. All Plaintiffs who incurred unauthorized charges suffered actual harm regardless of whether the charges were reimbursed because the charges are evidence of misuse and underscore the imminent, certainly impending further injury Plaintiffs face. And virtually all such Plaintiffs also allege closely related injuries, including loss of access to their account funds. None of the Plaintiffs whose accounts were restricted was reimbursed for the resulting loss of use of their funds. ¶ 119.

Target's challenge to Plaintiffs who lost access to their account funds defies both the facts and common sense. Target claims that "something more" is required for Article

---

[6] Plaintiff Julie Melnichuk incurred approximately 10 unauthorized charges, lost access to her account, incurred unreimbursed interest on the unauthorized charges and incurred unreimbursed late payment fees due to failed automatic payments. ¶ 20. Plaintiff Adba Quillian incurred multiple unauthorized charges totaling approximately $5,600 in January 2014, for which she was not fully reimbursed; lost access to her funds; and incurred late payment fees due to failed automatic payments. ¶ 33.

III injury, citing *Barnes & Noble*, which, as already discussed, is factually distinguishable. The court in *Barnes & Noble* denied standing where the plaintiff failed to allege injury from lack of credit card access. Plaintiffs who lost access to their money as a result of the Target breach state cognizable injuries flowing directly from loss of access to their money.

Although not required to do so, these Plaintiffs clearly allege the "something more." For example, Plaintiff Keller incurred fraudulent charges that were not reimbursed for more than two weeks, and because she was locked out of her account was unable to pay bills, resulting in unreimbursed late fees and missed bill payments. ¶ 1.a. *See also, e.g.*, ¶ 1.c. (Plaintiff Oliver had $1,506.98 in unauthorized charges, her bank account was partially frozen, causing her to miss a mortgage payment, and she incurred an unreimbursed late fee); ¶ 1.d. (Plaintiff Rhodes incurred an unauthorized charge, found his account frozen, resulting in missed bill payments and unreimbursed late fees, and incurred unreimbursed card replacement fees); ¶ 1.e. (Plaintiff Smart suffered multiple injuries, including loss of access to his funds and restrictions placed on his account); ¶ 1.g. (Plaintiff Reynoso's account was frozen from December 28 until January 14, leaving her no source of funds to care for her son).

Target quibbles that these Plaintiffs do not allege who canceled or restricted access to their accounts, or why. It is irrelevant for standing purposes whether a consumer or her bank canceled an account. Either way, the cancellation was necessitated by the breach. Plaintiffs' multiple actual injuries, including loss of access to their account funds, constitute classic consumer injury. *See F.T.C. v. Wyndham Worldwide Corp.*, No. 13-

1887 (ES), 2014 WL 1349019, at *16-17 (D.N.J. April 7, 2014) (denying motion to dismiss FTC claims that defendant engaged in unfair and deceptive practices in failing to safeguard customers' personal information and crediting FTC's allegations that consumers suffered substantial financial injury in multiple forms, including unreimbursed fraudulent charges, increased costs, lost access to funds or credit, and time and money spent resolving fraudulent charges and mitigating subsequent harm).

3. Identity Theft.

Contrary to Target's position, Plaintiffs Frederick Smart (¶ 1.f.) and Terry Dorsch (¶ 16), like all Plaintiffs, plead facts establishing their standing. Mr. Smart alleges that his Target REDcard was compromised as a result of the breach, that he incurred fraudulent charges ($101 in November, $277 in December), that he lost access to his funds, that he had to purchase credit monitoring services, that restrictions were placed on his account, and that 35 fraudulent inquiries caused his credit score to drop, forcing him to delay purchasing a new car. ¶ 1.f. Ignoring all these injuries, Target seizes on Mr. Smart's allegation that scammers opened phony accounts in his name and that he received scam telephone calls and mail, arguing that it suggests Mr. Smart's identity theft resulted from "his interactions with a third-party criminal," not from Target's conduct. Def.'s Mem. at 12. With or without this allegation, Plaintiff Smart has more than adequately pled injury.

Target also isolates Mr. Dorsch's allegation that he experienced identity theft when his social security number was stolen, arguing that Plaintiffs do not generally allege that social security numbers were stolen. Whether or not other Plaintiffs make the same

allegation is irrelevant. Dorsch does allege that Target's wrongdoing allowed his SSN to be stolen and used to open a new bank account and file a fraudulent tax return. ¶ 16.

4. Damages and Diminution in Value of Plaintiffs' Stolen Personal and Financial Information.

Target argues that personal information has no value fails for several reasons. First, Plaintiffs amply allege facts to support their allegation that the stolen information does indeed have significant value. ¶¶ 213-226. That hackers go to great lengths to steal and sell the information itself demonstrates value. More importantly, the Complaint alleges that the stolen information was actually marketed and sold on the black market. Batches of fake credit cards were sold at prices ranging from $20 to $100 per card. ¶ 224. Indeed, the very existence of this underground market evidences value. ¶ 222.

Target's own practices further demonstrate value. It collects extensive personal information from its customers and uses it to develop sophisticated marketing programs. ¶¶189-190. The FTC also recognizes the value that consumer financial and personal information holds for thieves. ¶ 214-215.

Contrary to Target's argument, Plaintiffs need not allege they attempted to sell their personal information or were prevented from doing so as a result of Target's conduct. Their standing is anchored in the allegations they do make.[7]

[7] *In re Google Android Consumer Privacy Litigation*, No. 11-MD-02264 JSW, 2013 WL 1283236 (N.D. Cal. March 26, 2013), cited by Target, is quite different from this case. In *Google*, the plaintiffs alleged the defendant improperly collected personal information without providing proper notice or obtaining consent. *Id*. at *1-2. The court denied standing because it found that plaintiffs did not allege actual harm resulting from

5. Injury From Target's Nondisclosure of Material Facts and Overcharges.

Plaintiffs allege that they would not have made purchases at Target using a credit or debit card – and would not have made purchases at all at Target during the breach – had Target disclosed that it lacked adequate security and properly notified them of the breach. ¶¶ 1.g., 115. Plaintiffs further allege that they were overcharged for purchases made at Target using their payment cards because a portion of the purchase price included the cost of adequate safeguards. As a result, Plaintiffs did not receive what they paid for and were overcharged. ¶ 117.

Target's argument that these allegations do not support standing is undermined by the very opinion it relies on. In *Grigsby v. Valve Corp.*, No. CV-0553JLR (W.D. Wash. March 18, 2013) (Wildung Decl., Ex. 1, ECF No. 208-1), the plaintiff sought damages after hackers breached the defendant's internet security system. The court ruled that the plaintiff had sufficiently alleged injury to his business or property "by asserting that had he known that Valve was not reasonably protecting the personal and private information that Mr. Grigsby provided to Valve for the purpose of purchasing Valve's products, he would not have paid the price he did for the products or would not have purchased the products at all." *Id.*, slip op. at 8.

---

access to the information. *Id*. at *4-6. Plaintiffs here amply allege actual harm resulting from the Target data breach. Also, the plaintiffs in *Google* alleged that they lost the opportunity to profit from their information but none alleged that they attempted to sell their personal information. *Id*. at *4. Here, Plaintiffs need not make such allegations.

Target also relies on *Remijas*, where the court rejected the plaintiffs' overcharge theory of harm. Without citing any authority, the court suggested that this theory of injury is available only where a deficiency is "intrinsic" to the product purchased, not where the deficiency is "extrinsic" to the product. 2014 WL 4627893, at *5. The court conceded that precedent, including a decision of the Seventh Circuit, made no such distinction. *Remijas*, at *4 (citing *In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) ("The plaintiffs' loss is financial: they paid more for the toys than they would have . . . ."). Target's failure to disclose that it did not have reasonable safeguards and data security in place and its failure to disclose the data breach in a timely and proper manner were material and influenced consumers' purchasing decisions. ¶¶ 1.f., 115, 227-231.

Other data breach cases have recognized this basis for standing. *See In re LinkedIn User Privacy Litig.*, No. 5-12-CV03088-EJD, 2014 WL 1323713, at *6 (N.D. Cal. March 28, 2014) (recognizing standing under California's Unfair Competition Law based on plaintiff's allegations that had defendant disclosed its lax security practices, plaintiff would have attempted to purchase defendant's product at a lower price or not at all); *Sony*, 996 F. Supp. 2d at 991 (denying motion to dismiss plaintiffs' California consumer law omission claims and finding standing where plaintiffs alleged they would not have purchased, or would not have paid as much for, defendant's products had defendant disclosed that its online services were not reasonably secure and did not conform to industry standards); *Adobe*, 2014 WL 4379916, at *15-16 (finding plaintiffs had standing to bring injunctive claim under California's Unfair Competition Law based on allegations

that they spent more on defendant's products than they would have had they known that Adobe was not providing reasonable security).[8]

Target further challenges Plaintiffs' overcharge injury theory on grounds that "[i]f Target charges a cash customer and a payment card customer the same amount for a given product, then there can be no overcharge." Def.'s Mem. at 14-15. Target's point is entirely irrelevant. Whether payment card customers pay "extra" for data security services is not the issue. Plaintiffs allege that built into the price of *all* products charged to *all* customers is a component reflecting Target's costs for providing adequate data security measures to all of its customers. Courts recognizing standing based on overcharge allegations have not insisted on any differential between pricing for credit and cash purchases. *See LinkedIn*, *Sony*, *Adobe*.[9]

6. Theft of Plaintiffs' Financial and Personal Information.

Amazingly, Target contends that the theft of Plaintiffs' sensitive data does not constitute an injury sufficient to confer standing. It is a bedrock principle of American jurisprudence that deprivation of property gives rise to a cognizable claim. Historically,

---

[8] Target's attempt to recast these decisions along the distinction made in *Remijas* between "intrinsic" and "extrinsic" deficiencies is strained and offends logic. There is no discussion of such a distinction in these decisions. Rather, they rest on established standing and consumer law principles.

[9] For these reasons, the reasoning of *Barnes & Noble*, cited by Target, should be rejected. The issue is not whether some "additional value" is expected by consumers using a credit card. All Plaintiffs would not have purchased at Target had it disclosed its inadequate security and provided timely and adequate notice of the breach, and all Plaintiffs were overcharged because they did not receive the value they paid, the component of Target's pricing allocated to providing adequate security.

courts have consistently held that loss of property or of a property interest is sufficient injury to confer Article III standing. *See, e.g.*, *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003, 1010-12 (1992) (plaintiff properly alleged injury-in-fact based on allegations government took his beachfront property by restricting building on it); *Martin Marietta Materials, Inc. v. City of Greenwood, Mo.*, No. 06-0697-CV-W-DW, 2007 WL 5193732, at *2 (W.D. Mo. Jan. 22, 2007) (plaintiff had standing based on her property interest in contract allegedly breached by defendant); *St. Charles Tower, Inc. v. Cnty. of Franklin, Mo.*, No. 4:09CCV987-DJS, 2010 WL 743594, at *3 (E.D. Mo. Feb. 25, 2010) (intervenors had standing based on allegations of diminished value to their property resulting from construction of telecommunications tower); *Hodel v. Irving*, 481 U.S. 704, 711 (1987) (deprivation of a fractional interest in land plaintiffs would have inherited but for a challenged federal statute sufficient to confer standing). And property interests may be found in the terms of express or implied contracts. *Ikpeazu v. Univ. of Neb.*, 775 F.2d 250, 253 (8th Cir. 1985). *See also Kwikset Corp. v. Superior Court*, 246 P.3d 877, 885-86 (Cal. 2011) (noting that "[t]here are innumerable ways in which economic injury from unfair competition may be shown," including a plaintiff being "deprived of money or property to which he or she has a cognizable claim"). Additionally, the theft of Plaintiffs' personal information is the predicate for the additional, multiple injuries Plaintiffs suffered as a direct result of the breach.

7. Stress, Nuisance and Annoyance in Dealing with the Aftermath of the Target Data Breach.

Plaintiffs allege as part of their multiple injuries the costs and loss of productivity

associated with addressing the consequences of the breach, including finding fraudulent charges, canceling and reissuing cards, purchasing credit monitoring, the imposition of withdrawal and purchase limits on compromised accounts and the "stress, nuisance and annoyance of dealing with all issues resulting from the breach in the weeks leading up to and beyond the holiday season." ¶¶ 2.e., 261(e). These allegations refute Target's assertion that Plaintiffs do not make "particularized allegations" to support these injuries. Based on the allegations of harm and suffering detailed in the Complaint, a jury could reasonably conclude that Target's conduct resulted in financial injury, stress, nuisance and annoyance as consumers were compelled to deal with the aftermath of the breach. *See F.T.C. v. Wyndham Worldwide Corp.*, 2014 WL 1349019, at *16-17 (recognizing FTC's claims that consumers suffered substantial financial injury as result of defendant's alleged failure to secure their data, including time and money spent resolving fraudulent charges and mitigating subsequent harm).

E. Plaintiffs Have Standing to Seek, and Are Entitled to, Injunctive Relief.

1. Plaintiffs Have Pled a Sufficient Basis for Injunctive Relief

Plaintiffs adequately plead and are entitled to injunctive relief under consumer protection laws, data protection and data breach notification statutes, and the Court's equitable powers.

Plaintiffs have alleged the requisites for injunctive relief, including impending future harm. Target continues to maintain Plaintiffs' personal information and has demonstrably failed to adequately protect it. The threat of additional breaches is not speculative – Target's security system has already proven ineffective. ¶¶ 200-212, 236.

See, e.g., *Sony II*, 996 F. Supp. 2d at 999 (injunctive relief appropriate where plaintiffs "alleged that Sony's network security is still inadequate"). In the years leading up to the breach, Target ignored repeated warnings of the inadequacies of its systems and the consequences of a breach to consumers. ¶¶ 128-131, 200-212. Plaintiffs seek an order that Target undertake appropriate measures to maintain security sufficient to prevent future breaches, such as encrypting sensitive consumer information, complying with the Payment Card Data Security Standard and Minn. Stat. § 325E.64, and utilizing EMV chip technology. Compl., Prayer for Relief C.

Plaintiffs further allege that Target, upon being alerted by its security systems that its computers had been infected with malware, did not notify its customers of the breach accurately and promptly. ¶¶ 175-178, 180, 270-78, 348. Requiring Target to implement policies that ensure data protection safeguards and timely notice of future breaches is an appropriate injunctive remedy to reduce the threat of future harm to Plaintiffs and Target's customers nationwide.[10]

2. State Data Breach Statutes and Consumer Laws Provide for Injunctive Relief.

Target's argument that injunctive relief is foreclosed by applicable law should also be rejected. First, the data breach statutes in five states expressly create a private right of

[10] As Target does here, General Mills argued in *Ebert v. General Mills, Inc.*, No. 13-3341, 2014 WL 4384462, at *4 (D. Minn. Sept. 4, 2014), that it had already taken remedial measures to address the alleged harm to the plaintiffs. The court rejected that argument at the motion to dismiss stage, crediting the plaintiffs' competing allegation that the defendant's remedial efforts were insufficient to mitigate the threat of future harm. *Id*.

action for injunctive relief.[11] Second, state consumer protection laws in 37 jurisdictions expressly permit plaintiffs to obtain injunctive relief (or equitable relief generally) for claims of unlawful, unfair and deceptive trade practices, and Plaintiffs have alleged Target's failure to maintain data security as a basis for violation of those laws.[12] ¶ 262. In fact, some data breach statutes expressly declare that they are enforceable through the state's consumer law.[13] In addition, a violation of a state data breach or customer data security law may constitute an unlawful act under state consumer protection laws regardless of whether the data breach law provides a private right of action. *See, e.g., Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 973 P.2d 527, 539-40 (Cal. 1999) ("[Cal. Bus. & Prof. Code § 17200] 'borrows' violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable") (citations and internal quotation marks omitted); *Chabner v. United of Omaha Life Ins. Co.*, 225 F.3d 1042, 1048 (9th Cir. 2000) ("It does not matter whether the underlying statute also provides for a private cause of action; section 17200 can form the basis for a private cause of action even if the predicate statute does not.").

3. The Court Has Broad Equitable Powers to Provide Injunctive Relief.

Some data breach statutes are either silent regarding injunctive relief or permit the state attorney general to pursue an injunction.[14] None of these statutes, however, prohibits

---

[11] *See* Pls.' App., Ex. B, Table 1.
[12] *See* Pls.' App., Ex. B
[13] *See* Pls.' App., Ex. B, Table 1.
[14] *See* Pls.' App., Ex. B, Table 1 and 2.

a court from awarding injunctive relief to a private litigant under its equitable powers.

Courts have broad equitable powers to fashion appropriate relief for statutory violations, including injunctions, where a statute does not expressly authorize it. *United States v. Oakland Cannabis Buyers' Co-Op*, 532 U.S. 483, 496 (2001) ("[W]hen district courts are properly acting as courts of equity, they have discretion unless a statute clearly provides otherwise. . . . Such discretion is displaced only by a clear and valid legislative command.") (internal citations and quotations omitted). "When a statute does not abrogate the traditional equitable discretion of the court," injunctive relief is available. *Osthus ex rel. N.L.R.B. v. Laborers Dist. Council of Minn. & N.D.*, 742 F. Supp. 2d 1042, 1047 (D. Minn. 2010). Accordingly, in the absence of language prohibiting injunctive relief, courts may award it to vindicate important public interests. *Action v. Gannon*, 450 F.2d 1227, 1237-38 (8th Cir. 1971) (holding that district court had the authority to grant injunctive relief under 42 U.S.C. § 1985(3), even though statute only provided for an award of damages).

States have enacted important laws requiring Target to secure customer data. *See, e.g.*, Cal. Civ. Code. § 1798.81.5 ("A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."); *see also* Ark. Code Ann. § 4-110-104(b); Fla. Stat. Ann. § 501.171(2); Md. Code Ann., Com. Law § 14-3503; Mass. Gen. Laws Ann. Ch. 93H § 2(a); Nev. Rev. Stat. Ann. § 603A.210 & 215; N.C. Gen. Stat. Ann. § 75-62(c); Or. Rev. Stat. Ann. § 646A.622; R.I.

Gen. Laws Ann. § 11-49.2-2; Tex. Bus. & Com. Code Ann. § 521.052; Utah Code Ann. § 13-44-201(1). Other states have emphasized the importance of protecting sensitive personal information. *See, e.g.*, Mont. Code Ann. § 30-14-1701 ("The purpose of 30-14-1701 through 30-14-1705, 30-14-1712, and 30-14-1713 is to enhance the protection of individual privacy and to impede identity theft"); *see also* Ga. Code Ann. § 10-1-910; La. Rev. Stat. Ann. § 51:3072; N.H. Rev. Stat. Ann. § 359-C:2.

Injunctive relief enforcing states' legislative aims by requiring Target to maintain security standards to prevent future breaches is important because Target continues to maintain troves of customer data coveted by criminals, and has failed to adequately protect it. Injunctive relief will enforce the public policy behind these laws, which will benefit the tens of millions of customers impacted by Target's conduct.

F. Target's Challenge to Plaintiffs' Standing to Sue for Violations of Particular State Laws Is Premature and Wrong.

Target argues that Plaintiffs cannot assert claims under the laws of Delaware, Maine, Rhode Island, South Carolina, Wyoming or the District of Columbia because none of the named Plaintiffs resides in those jurisdictions. Target's argument is both premature and wrong as a matter of law. It is premature because it presents a Rule 23 issue that will not be before the Court until Plaintiffs move for class certification. It is wrong, first, because Target confuses Article III standing with class standing. There is no requirement under governing class (or Article III) standing principles that a named plaintiff have the exact same claim, or suffer the exact same injury, as absent class members. Instead, Target's position is contrary to Supreme Court precedent and the plain

language of Rule 23, as reflected in the vast majority of cases that have analyzed this issue.

The overwhelming majority of courts follow *Ortiz* to hold that Article III standing under state statutes should 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); *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").[15]

---

[15] Courts in at least eleven jurisdictions reach the opposite conclusion from the one reflected in the two cases Target cites. *See 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."); *Edwards v. 21st Century Ins. Co.*, No. 09-04364, 2010 WL 2652247, at *4 (D.N.J. June 23, 2010) ("Defendants conflate the inquiry into Plaintiff's standing to bring her claims with the separate question of whether a class representative may bring claims on behalf of class members when the claims are based on slightly different facts from those experienced by the class representative."); *Ramirez v. STi Prepaid LLC*, 644 F. Supp. 2d 496, 505 (D.N.J. 2009) ("Defendants' argument appears to conflate the issue of whether the named Plaintiffs have standing to bring their individual claims with the secondary issue of whether they can meet the requirements to certify a class under Rule 23. . . . The Complaint makes clear that the so-called "sister state" consumer protection laws are only implicated by members of the putative class. . . . Hence, the fact that the named Plaintiffs may not have individual standing to allege violations of consumer protection laws in states other than those in which they purchased Defendants' calling cards is immaterial."). *See also Saltzman v. Pella Corp.*, 257 F.R.D. 471, 480 (N.D. Ill. 2009), *aff'd*, *Pella Corp. v. Saltzman*, 606 F.3d 391 (7th Cir. 2010); *In re Auto. Parts Antitrust Litig.*, No. 12-md-02311, 2013 WL 2456612, at *11-12 (E.D. Mich. June 6, 2013); *Owens v. Apple, Inc.*, No. 09-cv-0479-MJR, 2009 WL 5126940, at *4 (S.D. Ill. Dec. 21, 2009); *In re Chocolate Confectionary Antitrust Litig.*, 602 F. Supp. 2d 538, 579-80 (M.D. Pa. 2009); *Young v. Wells Fargo & Co.*, 671 F. Supp. 2d 1006, 1023-24 (S.D. Iowa

Target's position is also wrong because federal courts routinely certify classes under the laws of multiple states even where there is not a plaintiff from every state. *See, e.g., Bussie v. Allmerica Fin. Corp.*, 50 F. Supp. 2d 59, 63-64, 71 (D. Mass. 1999) (nationwide class certified under laws of 50 states with class representatives from Louisiana); *Shaw v. Toshiba Am. Info. Sys.*, 91 F. Supp. 2d 942, 953, 956-57 (E.D. Tex. 2000) (certifying class under laws of 50 states with two named plaintiffs); *Duhaime v. John Hancock Mut. Life Ins. Co.*, 177 F.R.D. 58, 62, 64 (D. Mass. 1997) (certifying class under laws of 50 states with five named plaintiffs).

Alternatively, if this Court adopts the narrower minority position reflected in *Insulate SB, Inc. v. Advanced Finishing Systems*, No. 13-2664, 2014 WL 943224 (D. Minn. Mar. 11, 2014), relied upon by Target, then Plaintiffs respectfully request leave to amend to include plaintiffs in those jurisdictions now missing a named plaintiff. That additional plaintiffs may be added through the date for adding additional parties or the amendment process underscores the fact that this issue is truly one of class certification and should properly be deferred to that stage.

2009); *Woodard v. Fid. Nat'l Title Ins. Co.*, No. 06-cv-1170, 2007 WL 5173415, at *3-4 (D.N.M. Dec. 4, 2007); *Jepson v. Ticor Title Ins. Co.*, No. 06-1723-JCC, 2007 WL 2060856, at *2 (W.D. Wash. May 1, 2007); *In re Relafen Antitrust Litig.*, 221 F.R.D. 260, 267-70 (D. Mass. 2004); *Ferrell v. Wyeth-Ayerst Labs., Inc.*, No. C-1-01-447, 2004 WL 6073010, at *3-4 (S.D. Ohio, June 30, 2004).

V. CONSUMER LAW CLAIMS

A. Plaintiffs Have Adequately Alleged Claims for Violations of the Consumer Protection and Unfair Practices Statutes.

Plaintiffs have pled the facts, law, nexus, and damages necessary to sustain claims that Target violated the various state consumer protection and unfair practices statutes. These statutes cover and provide remedies for Target's failure to safeguard consumers' private data.

B. Plaintiffs Need Not Have Class Representative Plaintiffs from Each State in Order to Raise Claims under the Statutes of Such State.

Target's argument is addressed in Part IV.F. Additionally, the cases Target cites do not support its challenge to Plaintiffs' consumer law claims. *Allstate Insurance Co. v. Hague*, 449 U.S. 302, 312-13 (1981) strongly suggests Plaintiffs *can* bring claims on behalf of citizens of all 50 states and the District of Columbia. The connections between the case and the state at issue are at least as extensive here as those in *Allstate*, where it was enough that the insured decedent worked in Minnesota, the defendant was present and doing business in Minnesota, and the plaintiff was not forum shopping when she relocated to Minnesota. *See id.* at 313-320. Delaware, Maine, Rhode Island, South Carolina, Wyoming, and the District of Columbia all have at least one Target store and collectively have 34. Target does business in those states; there are tens if not hundreds of thousands of Target shoppers in each state whose claims are pursued in this case, and there is no question that customers' personal information was stripped from Target point-of-sale machines in each state. It would be "neither arbitrary nor fundamentally unfair"

for Target to be subject to the laws of the states where it collected but failed to protect consumers' sensitive financial and personal data.

In re Bridgestone/Firestone, Inc., Tires Products Liability Litigation, 288 F.3d 1012, 1018 (7th Cir. 2002), is not a decision applying Rule 12, but rather a Rule 23(f) review of a class certification order. Moreover, the language Target quotes concerns applying one state's laws to another state's sales. That is *not* what Plaintiffs seek to do here. Instead, they seek to apply the laws of each state and assert claims on behalf of separate statewide classes (and, as to REDcard holders, on behalf of nationwide class based on South Dakota law). Far from indicating Plaintiffs' claims should be dismissed, *Bridgestone* suggests only that state-by-state claims should be brought, which is exactly what Plaintiffs have done.

Finally, Target invokes *Mazza v. American Honda Motor Co.*, 666 F.3d 581, 596 (9th Cir. 2012), another inapposite class certification decision. That *Mazza* may suggest California consumer protection laws should not apply to out-of-state residents has no bearing here where Plaintiffs seek to apply the laws of each state to the claims of the residents of those states.

C. Plaintiffs Adequately Plead Injuries.

Target asserts that the consumer protection statutes of 26 states require a higher standard for pleading injury than Article III does. Target is mistaken. Its cursory review of those statutes' remedial provisions ignores the attending case law. Of the state consumer protection and unfair practices statutes Target cites, 15 contain language that courts in their home jurisdictions have expressly construed to include non-pecuniary

losses.[16] Of the remaining nine statutes, seven expressly or by judicial construction mandate liberal or broad construction.[17] And the remaining two states' laws instruct the court to construe the acts in accordance with federal law.[18]

As an illustration, Target has clumped together every statute containing remedial provisions for Plaintiffs with "ascertainable losses" and construed that language to require a direct and strict pecuniary loss. Kentucky is one of the states containing "ascertainable loss" language, but the Kentucky Supreme Court has rejected Target's interpretation, awarding damages for future promises of financing, absences from work, inconvenience, and "constant telephoning." *Craig & Bishop, Inc. v. Piles*, 247 S.W.3d 897, 907 (Ky. 2008). Oregon also requires "ascertainable loss,"[19] but its court of appeal has held that "[a]ny loss will satisfy [the ascertainable loss] requirement so long as it is capable of being discovered, observed, or established." *Feitler v. Animation Celection, Inc.*, 13 P.3d 1044, 1050 (Or. Ct. App. 2000) (citing *Scott v. Western Int'l Sales, Inc.*, 517 P.2d 661, 663 (Or. 1973) (internal quotations omitted). *See also id.* at 1047 ("ascertainable loss requirement should be 'viewed broadly' and that losses too small to be cognizable under the common law nevertheless suffice for purposes of the UTPA"). This law refutes Target's characterization of the statutes.

---

[16] The consumer statutes are: Connecticut, Idaho, Iowa, Kentucky, Louisiana, Mississippi, Missouri, Montana, New Jersey, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, and West Virginia. *See* Pls.' App., Ex. A.

[17] *See* Pls.' App., Ex. A.

[18] Alabama's and Nebraska's consumer laws. *See* Pls.' App., Ex. A.

[19] Or. Rev. Stat. § 646.638.

Thirteen additional state consumer protection statutes lumped together by Target share Kentucky and Oregon's "ascertainable loss" language, and many of the states' jurisdictions have explicitly construed them contrary to Target's restrictive definition. These states include Tennessee,[20] Connecticut,[21] Idaho,[22] and New Jersey.[23] Target offers no case law supporting a restrictive construction that nearly half the states have rejected.

The nine remaining statutes that do not use the phrase "ascertainable loss," but are still in Target's pecuniary loss category, contain remedial provisions with diverse language. Seven of these statutes have clauses or interpreting case law requiring liberal construction, but Target has construed each of them to have precisely the same cramped meaning.[24] With the exception of a single inapposite case construing California law, discussed below, Target offers no analysis of these individual states' provisions and no case law to show how that language is meant to be construed. Target bears the burden of proving its novel and highly restrictive construction of 24 statutory provisions meant to broadly protect consumers. Given the judicial constructions that explicitly repudiate Target's view of those statutes, and given Target's misguided attempt to squeeze diverse,

---

[20] *Discover Bank v. Morgan*, 363 S.W.3d 479, 495 (Tenn. 2012) (holding that ascertainable loss includes reduction in credit rating).

[21] *Serv. Rd. Corp. v. Quinn*, 698 A.2d 258, 262-63 (Conn. 1997).

[22] *In re Wiggins*, 273 B.R. 839, 856 (Bankr. D. Idaho 2001) ("Ascertainable loss is defined under the Idaho Rules of Consumer Protection to include . . . : [a]ny deprivation, detriment, or injury, or any decrease in amount, magnitude, or degree that is capable of being discovered, observed, or established." (Internal quotation marks omitted)).

[23] *Thiedemann v. Mercedes-Benz USA, LLC*, 872 A.2d 783, 792-793 (N.J. 2005).

[24] *See* Def.'s Mem. at 20. *See also* Def.'s Mem. App. A.

liberally construed statutes into a single restrictive meaning, Target fails to shoulder its burden.[25]

In sum, the Complaint easily meets all state consumer law standards by alleging ten categories of pecuniary, economic, ascertainable injuries, many of which are readily measurable and identifiable even under the "economic injury" rubric that Target suggests. ¶ 261. Target ignores these allegations and provides no analysis showing how they fail to meet the pleading standards. Instead, it merely floats *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012), which held that the plaintiffs failed to meet the California "economic injury" pleading standard because they had not sufficiently pled the injury theories particular to the facts of that case. Having failed to show how this lone case, decided solely under California law, applies to Plaintiffs' many allegations of injuries, Target again fails to carry its Rule 12(b)(6) burden.[26]

D. Target's Duty-to-Disclose Argument Involves Only a Small Subset of Plaintiffs' Claims and Is Wrong as a Matter of Law.

Target asks the Court to dismiss all or part of claims under nine of the consumer protection statutes on the grounds that, in order to properly plead deception-by-omission,

---

[25] *See* Pls.' App., Ex. A.

[26] Target's claim that *Sony* dismissed claims under Florida, Michigan, New Hampshire, New York, and Texas law is incorrect. The decision was entirely concerned with California cases interpreting California statutes and California's Proposition 64. No other state statutes were mentioned.

Plaintiffs must plead a "duty to disclose."[27] Target admits that nine of these statutes permit claims for more than just "deceptive" conduct and thus seeks to dismiss only "the portion of Plaintiffs' UDAP claims based on deceptive conduct." Def.'s Mem. at 22.[28] In essence, Target argues that Plaintiffs must plead *every* element of fraud under *each* of the 18 states' common law regimes in order to show fraud-by-omission under their statutes. In support of that argument, Target cites two Minnesota cases applying Minnesota law, both holding the opposite of what Target proposes. *Graphic Communications Local 1B Health & Welfare Fund A v. CVS Caremark Corp*., 850 N.W.2d 682 (Minn. 2014) held "that a plaintiff bringing an action under the [Minnesota's] CFA must plead and prove not only an omission of material fact, but also special circumstances that trigger a duty to disclose." *Id.* at 696-97 (dismissing claims because plaintiffs "failed to allege any facts that would trigger a duty for the Pharmacies to disclose additional facts"). As discussed above, Plaintiffs have pled abundant facts giving rise to a duty to disclose material information, including allegations that Target knew its customers' data is sensitive and must be protected, continued to accept payment cards with actual or constructive knowledge that their systems were susceptible to breach and had been breached, and had

[27] Target's argument addresses only the following states: Arizona, California (both statutes), Connecticut, Delaware, Hawaii (Consumer Protection Act only), Idaho, Kansas, Louisiana, Maryland, Michigan, Minnesota (Consumer Fraud Act only), Missouri, New Mexico, Nevada, Oklahoma, Texas, and Washington.

[28] Target argues that the Indiana Deceptive Consumer Sales Act does not apply to non-disclosures. Def.'s Mem. at 22 n.14. However, the statute expressly prohibits the commission of an "unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction." Ind. Code Ann. § 24-5-0.5-3(a). The statute clearly covers Target's conduct, including its omissions of material facts.

special knowledge of material facts, including that its systems were inadequate and that the breach was happening. *See*, *e.g.*, ¶¶ 232-235.

Target next argues that Plaintiffs must plead every element of common law fraud in each state requiring a duty to disclose in order to properly plead fraud under their respective consumer protection acts. In support, Target cites *Tacheny v. M&I Marshall & Ilsley Bank*, 10-CV-2067 PJS/JJK, 2011 WL 1657877 (D. Minn. Apr. 29, 2011). But the court in *Tacheny* did not dismiss the claims for failure to plead every element of fraud. Instead, it dismissed the claims for failure to plead *any deceptive omissions whatsoever*. *Id.* at *7. In contrast, Plaintiffs have alleged multiple acts and forbearances that constitute omissions under Minnesota law and the law of the nine consumer protection laws at issue in this argument. *See* ¶ 259. Additionally, Plaintiffs do not plead common law fraud but violations of state consumer laws, which are legislative responses to the inadequacies of the common law in protecting the public. Consumer law claims encompass more than common law. *See State ex rel. Hatch v. Fleet Mortg. Co.*, 158 F. Supp. 2d 962, 967 (D. Minn. 2001) (noting that the Minnesota Consumer Fraud Act and Uniform Deceptive Trade Practices Act "are broader than common law fraud"); *State by Humphrey v. Alpine Air Prods., Inc.*, 490 N.W.2d 888, 892 (Minn. Ct. App. 1992) ("Consumer protection laws were not intended to codify the common law" but "were intended to broaden the cause of action to counteract the disproportionate bargaining power present in consumer transactions.") *aff'd*, 500 N.W.2d 788 (Minn. May 21, 1993).

Target argues that certain consumer protection statutes in Delaware, Hawaii, Illinois, Maine, Minnesota, and Nebraska only allow injunctive relief. However,

Plaintiffs have pled other consumer protection provisions for each of these states and for the reasons set forth in Section IV.F., they adequately plead a basis for injunctive relief.

Plaintiffs acknowledge that there is no private right of action under the Delaware Deceptive Trade Practices Act or the Oklahoma Deceptive Trade Practices Act (and withdraw those claims only), but they also invoke consumer protection acts in both states that do provide private rights of action, which Target does not dispute. *See* Def.'s Mem. at 22.

E. Plaintiffs Are Entitled to Pursue a Class Action in All States.

In Alabama, Georgia, Louisiana, Mississippi, and South Carolina, the individual prohibitions on class actions are procedural components of the consumer protection statutes and are therefore preempted by Fed. R. Civ. P. 23. In *Shady Grove Orthopedic Associates, P.A. v. Allstate Insurance Co.*, 559 U.S. 393 (2010), the Supreme Court held that state prohibitions against class actions are procedural and that the "right . . . not to be subjected to aggregated class-action liability in a single suit" is not a substantive right. *Id.* at 408 (internal quotation marks omitted).

In *In re Hydroxycut Marketing and Sales Practices Litigation*, the court applied *Shady Grove* to claims for violation of 41 states' consumer protection statutes, including those in Georgia, Louisiana and South Carolina. 299 F.R.D. 648, 651 (S.D. Cal. 2014). The defendants argued that these prohibitions are not preempted by Fed. R. Civ. P. 23 because the limiting provisions are "found *within* the state consumer protection acts and are therefore so intertwined with state rights and remedies that application of Rule 23 would violate the Rules Enabling Act." *Id*. at 652. The court rejected the argument,

reasoning that prohibitions against class actions only affect "how the claims are processed" and "[t]he fact that the class action prohibitions are within the individual state consumer protection acts, as opposed to free-standing rules, does not alter the Court's conclusion." *Id.* at 654 (citing *Shady Grove*, 559 U.S. at 408).

Target also argues that the Kentucky CPA prohibits class actions based on a reading of *In re Pharmaceutical Industry Average Wholesale Price Litigation*, 230 F.R.D. 61, 84 (D. Mass. 2005). But the Sixth Circuit reversed the dismissal of a class action under that statute in *Corder v. Ford Motor Co*., 285 F. App'x 226, 229-30 (6th Cir. 2008), and a district court has since upheld a class action case under the statute. *Naiser v. Unilever U.S., Inc.*, 975 F. Supp. 2d 727, 741 (W.D. Ky. 2013). Both of these cases tacitly acknowledged that class actions are allowed under the Kentucky CPA.

Finally, Target asks the Court to dismiss Plaintiffs' Utah and Ohio claims on grounds that Plaintiffs failed to plead that the challenged acts were declared to be deceptive by courts in those jurisdictions. To do so, Target incorrectly implies that Plaintiffs concede (in Compl. ¶ 262(rr)) that they were unable to locate any similar acts previously declared to be deceptive. Compl. ¶ 262(rr) contains no such concession. Furthermore, Plaintiffs plead a host of Ohio cases declaring omissions similar to Target's were deceptive. ¶ 262.ii.

In summary, Plaintiffs' consumer protection law claims are well pled and should be sustained.

VI. PLAINTIFFS ADEQUATELY PLEAD CLAIMS FOR VIOLATIONS OF STATE DATA BREACH STATUTES.

Plaintiffs assert claims on behalf of proposed statewide classes for Target's violations of state data breach statutes in 35 states. These statutes require businesses owning or licensing computerized data that includes personal information to disclose any breach to any affected resident of the state. The statutes further require that the disclosure be made in the most expedient time possible and without unreasonable delay. ¶ 267. For example, the California Data Breach Act requires that disclosure of the breach "shall be made in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). Minnesota's statute has the same requirement. Minn. Stat. § 325E.61, subd. 1.

The Target data breach falls squarely within the meaning of these statutes. ¶¶ 268-269. Target unreasonably delayed informing affected persons about the breach after it knew or should have known the breach had occurred. ¶¶ 270-282. *See supra* at 4.

A. Plaintiffs May Sue for Violations of State Data Breach Laws.

Forty-seven states have data breach laws requiring businesses to provide timely notice of any security breach of their computerized data systems. These statutes fall into four categories based on their enforcement provisions. At one end of the spectrum are seventeen states whose statutes expressly provide for a private cause of action.[29] Target

[29] *See* Pls.' App., Ex. B, Table 1. Target only identified nine of these states. Its list, however, failed to account for statutes that provide a private right of action through the

does not contest Plaintiffs' ability to sue under these laws. At the other end of the spectrum are thirteen states whose data breach statutes provide for exclusive enforcement by the state attorney general or do not allow for a private remedy.[30] Plaintiffs do not assert claims under any of these statutes.[31] In the middle are (1) fourteen statutes providing that the attorney general may enforce the statute but using permissive, non-exclusive language in conferring that authority;[32] and (2) four that are silent regarding an enforcement mechanism.[33] Target's arguments for dismissal of Plaintiffs' claims under these two middle groups fail.

The fact that a state data breach statute is silent as to an enforcement mechanism, or provides for enforcement through a state official, does not prohibit a private remedy to effectuate the purpose and policy of the statute to protect consumers' data.[34] Private enforcement of these data breach statutes is both appropriate and necessary for several reasons.

---

state's consumer protection law. Plaintiffs have identified these states in Pls.' App., Ex. B.

[30] *See* Pls.' App., Ex. B, Table 4.

[31] Plaintiffs withdraw their claims under the data breach statutes of Florida, Oklahoma and Utah. Further research indicated these statutes should properly be categorized in Pls.' Ex. B, Table 4.

[32] *See* Pls.' App., Ex. B, Table 2.

[33] *See* Pls.' App., Ex. B, Table 3.

[34] For example, in non-exclusive language, the Minnesota statute directs the attorney general to enforce the statute: "The attorney general shall enforce this section and Section 13.055, subdivision 6, under section 8.31 [Minnesota's private attorney general statute]." Minn. Stat. § 325E.61, subd. 6.

First, data breach statutes are quintessential consumer protection laws. Their purpose is to protect sensitive consumer data. They are frequently codified within the state's consumer laws. For example, Minn. Stat. § 325E.61 is in a chapter devoted to consumer protection laws, including a wide range of trade practices statutes.[35] Consumer protection laws are a paradigm of remedial legislation entitled to a liberal construction. *See State v. Phillip Morris, Inc.*, 551 N.W.2d 490, 495-96 (Minn. 1996) (stating that the Consumer Fraud Act "reflect[s] a clear legislative policy encouraging aggressive prosecution of statutory violations" and therefore should be "generally very broadly construed to enhance consumer protection").

Second, had the legislatures intended the designation of attorney general enforcement authority to be exclusive, or that silence on remedies bars private enforcement, the legislatures could have said so.

Third, once more using Minnesota's statute for illustrative purposes, there is no need for the statute to specifically provide a private remedy, for two reasons. The first is that Minn. Stat. § 325.E.61, subd. 6, directs the state attorney general to enforce the statute under § 8.31. Minn. Stat. § 8.31 authorizes the attorney general to prosecute violations of "the law of this state respecting unfair, discriminatory, and other unlawful practices in business, commerce, or trade, and specifically, *but not exclusively*, the [list of

[35] Minnesota's data breach statute is found in Ch. 325E, which regulates a host of diverse trade practices and is sandwiched between Ch. 325D (containing numerous unfair discrimination and competition statutes, including the Uniform Deceptive Trade Practices) and Ch. 325F (codifying a series of consumer protection statutes governing products and sales practices).

identified statutes].” (Emphasis added). Section 8.31, subd. 3a, creates a private remedy, authorizing “any person injured by a violation of any of the laws referred to in subdivision 1” to bring a civil action. Construing § 8.31’s *non-exclusive* listing of statutes governing unfair, discriminatory and other unlawful practices pursuant to its plain language and the liberal construction to which it is entitled, Minn. Stat. § 325E.61 clearly falls within its reach.

The other reason is that there is an existing private remedy for damages for persons injured by violations of the MGPDA. The reference in § 325E.61, subd. 6, authorizing the attorney general to enforce “this section and section 13.055, subd. 6 under § 8.31” is to a provision in the Minnesota Government Data Practices Act requiring notice in the event of breach of data maintained by a state agency. Minn. Stat. § 13.055. That statute provides for a private remedy. Minn. Stat. § 13.08. Under a basic principle of statutory construction, Minn. Stat. § 645.16-645.17, § 325E.61, subd. 6, should be construed to avoid the unreasonable result of denying a private remedy to injured persons when data held by private businesses is compromised but allowing them to sue when data maintained by a state agency is breached.

Fourth, a useful parallel is *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 381 n.23 (1982), where the Supreme Court held that a section of the Fair Housing Act permitting the Attorney General to bring a civil action challenging a “pattern or practice” of unlawful conduct was “only to describe the suits that the Attorney General may bring, and not to limit suits that private parties may bring.” In the same way, statutes like

Minnesota's should be read as describing the state official's authority to sue without denying injured consumers the right to bring an action.

Fifth, violations of state data breach laws are encompassed within state consumer laws prohibiting unfair methods of competition or unfair or deceptive trade practices. *See, e.g., In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 526 (N.D. Ill. 2011) (holding that customers' allegations that defendant violated Illinois Personal Information Protection Act by failing to timely notify affected customers of security breach were sufficient to state claim under Illinois Consumer Fraud and Deceptive Trade Business Practices Act); *Graphic Commc'ns Local 1B Health & Welfare Fund "A" v. CVS Caremark Corp.*, 850 N.W.2d at 693-94 (holding that injured person was permitted to bring consumer fraud claim under Minnesota's Consumer Fraud Act for damages under Private Attorney General Statute, Minn. Stat. § 8.31, for conduct that violated pricing provision of Pharmacy Practice Act, which itself did not afford private remedy). Thus, a violation of a state data breach statute may constitute an unlawful act under state consumer protection law regardless of whether a plaintiff has a private right of action under the data breach law itself. *See* discussion and cases cited *supra*, at 30-31.

Sixth, the Supreme Court's recent decision in *Lexmark International, Inc. v. Static Control Components, Inc.*, 134 S. Ct. 1377 (2014), is instructive. In finding standing, the Court stated that "a statutory cause of action extends only to plaintiffs whose interests 'fall within the zone of interests protected by the law invoked.'" *Id.* at 1388 (citation omitted). Plaintiffs injured by Target's violations of state data breach statutes clearly fall within the zone of interests and class of persons the legislatures intend to protect.

Recognizing a private remedy furthers the legislative purpose of protecting consumers by requiring businesses to safeguard their customers' data. *See, e.g.*, Cal. Civ. Code § 1798.81.5(a) (stating that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected" and that "the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information"). Granting a private remedy to the very persons whose personal information is safeguarded under data breach statutes effectuates legislative intent and serves the underlying public protection purposes.

B. Target's Remaining Arguments for Dismissal of Plaintiffs' State Data Breach Statutory Claims Also Fail.

Target argues that Plaintiffs have failed to allege that they suffered damages resulting from delayed or defective notice, as opposed to damages caused by the Target data breach itself. There is nothing in state data breach statutes making such a distinction. In any event, Plaintiffs have alleged damages flowing from the delay in notification itself. *See* ¶ 283. Specifically, had Target properly provided notice of the breach, Plaintiffs would have been able to avoid harm by refraining from credit or debit card purchases at Target stores or from shopping there at all, by cancelling their cards, and by otherwise attempting to avoid further harm. ¶ 284. Contrary to Target's unsupported contention, Plaintiffs have no obligation under Rule 8 to specify the exact date of their purchases or allege that their data was stolen before any notice was provided.

VII. PLAINTIFFS HAVE ALLEGED PLAUSIBLE NEGLIGENCE CLAIMS.

The elements of negligence are essentially uniform across all jurisdictions, consisting of: (1) a duty of care; (2) a breach of that duty; (3) causation; and (4) damages. *See* Pls.' App., Ex. C. Plaintiffs have adequately alleged plausible claims of negligence under the laws of their respective states.

A. Target Breached Its Duty of Care to Plaintiffs and Members of the Class.

Target does not persuasively deny that it owed Plaintiffs a legal duty of care to reasonably safeguard their personal information and to timely disclose the data breach. The case it relies on noted that the "duty to safeguard a consumer's confidential information entrusted to a commercial entity" is "well supported by . . . common sense . . . ." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d at 966. The court went on to observe that the "duty to safeguard a consumer's confidential information entrusted to a commercial entity" is well supported by both California and Massachusetts law. *Id*. (Citations omitted.) Other courts have also recognized the duty in data breach cases. *See, e.g., Sovereign Bank v. BJ's Wholesale Club, Inc*., 533 F.3d 162, 176 (3d Cir. 2008) (applying Pennsylvania law to hold that damages resulting from data breach were "foreseeable result of not taking appropriate precautions to protect . . . cardholders' 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 under California law); *Kahle v. Litton Loan Servicing LP*, 486 F. Supp. 2d 705, 708-709 (S.D. Ohio 2007) ("It is clear to the Court that Defendant owed a duty of care to the Plaintiff and that the duty was breached . . . .").

Target's duty is based in part on the fact, which cannot seriously be disputed, that Plaintiffs were foreseeable victims of its inadequate security system. ¶ 290; *See Fetterly v. Ruan Logistics Corp*., No. 12-2617 (PAM/JJK), 2013WL 6175181, at *3 (D. Minn. Nov. 25, 2013) (Magnuson, J.) (discussing factors supporting a duty of care, including "foreseeability of harm to the plaintiff").

Target also owed duties to Plaintiffs under industry standards and Minn. Stat. § 325E.64, subd.2, which prohibits Target from "retain[ing] the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction." ¶¶ 300-302. Target's persistent violations of this statute, as alleged in the Complaint, constitute evidence of negligence *per se*, which "substitutes a statutory standard of care for the ordinary prudent person standard of care, such that a violation of a statute . . . is conclusive evidence of a duty and breach." *Dillard v. Torgerson Props, Inc.*, No. 05-cv-2334, 2006 WL 2974302, at *4 n.2 (D. Minn. Oct. 16, 2006) (Magnuson, J.) (citations and internal quotation marks omitted).

Finally, duties of care also arise from the special relationship between Target and Plaintiffs. ¶¶ 306-309. Target agrees that a special relationship would give rise to such a duty. *See* ECF No. 221, at 3-4 (discussing Minnesota's "well-established" "special

relationship" test). A special relationship may exist, for example, where "the plaintiff is in some respect particularly vulnerable and dependent on the defendant, who in turn holds considerable power over the plaintiff's welfare." *Donaldson v. Young Women's Christian Ass'n of Duluth*, 539 N.W.2d 789, 792 (Minn. 1995).

That is precisely the case here. By entrusting their private information to Target, Plaintiffs became entirely dependent on Target to protect them. Target – *and only Target* – was in a position to prevent the harm they suffered. Target fully accepted this responsibility, as evinced by Target's Privacy Policy, which, as Target concedes in its recently filed reply brief in support of its motion to dismiss Financial Institutions Plaintiffs' Complaint, "is clearly directed . . . to consumers[,]" ECF No. 221, at 10.

Duty is ultimately a question of policy. *Erickson v. Curtis Inv. Co.*, 447 N.W.2d 165, 169 (Minn. 1989). "Imposing a duty on Target will further the policies underlying negligence law and encourage Target and other retailers to adopt, maintain and properly implement reasonable, adequate and industry-standard security measures to protect such customer information." ¶¶ 308-309.

Should Target rely on *Sony* to deny the existence of a special relationship, the case is easily distinguishable. *Sony* involved a data breach that caused a disruption in service to the popular Play Station Network ("PSN") – a free service that allows users to play multi-player online games. 996 F. Supp. 2d at 953-54. The plaintiffs' alleged damages included loss of use and value of the PSN, credit monitoring costs, and diminution in value of their gaming consoles. *Id.* at 968-69. The court, applying California law, found no special relationship between the parties because the plaintiffs' alleged damages were

not caused by Sony and were not foreseeable. *Id.* at 968-72. Specifically, the court reasoned that the PSN was offered free of charge and that in order to use the PSN, the plaintiffs entered into a contract with Sony that expressly disclaimed uninterrupted service. *Id.* at 969. With respect to the plaintiffs' credit monitoring costs, the court found that they were not reasonable or necessary absent any misuse of the plaintiffs' personal information. *Id.* at 970. Here, unlike in *Sony*, Plaintiffs allege actual theft and misuse of their private data, which was associated with their intended transaction (the purchase of goods) rather than the subject of the transaction itself.

B. Target's Negligence Caused Plaintiffs to Suffer Appreciable, Non-speculative Damages.

Unlike the facts in virtually all other data breach cases, Plaintiffs do not allege that they were damaged merely because their personal information was "exposed."[36] Rather, they allege non-speculative damages arising from the actual theft and misuse of their private information, evidenced by numerous unauthorized charges and costs incurred immediately after the breach, and the sale of their information on the black market. Target concedes that unauthorized charges constitute actual damages.[37] And in *RockYou*,

---

[36]*See, e.g.*, *Pisciotta v. Old Nat'l Bancorp*, No. 1:05-cv-668, 2012 U.S. Dist. LEXIS 160878, *2-3 (S.D. Ind. Sept. 19, 2012) (alleged injury caused by mere exposure of confidential information); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 275 (S.D.N.Y. 2008) (same); *Melancon v. La. Office of Student Fin. Assistance*, 567 F. Supp. 2d 873, 874 (E.D. La. 2008) (same); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1019-1020 (D. Minn. 2006) (same).

[37]Many of the costs Plaintiffs incurred have not been reimbursed, but to the extent that Target argues that Plaintiffs must allege "actual damages," they address that argument in Part IV.D.2.

the court held that the plaintiffs' personal information had value, denying a motion to dismiss a negligence claim on the ground that disclosure of the plaintiffs' personal information was insufficient to allege actual damages. 785 F. Supp. 2d at 866.

Finally, because Plaintiffs' personal information has actually been offered for sale on the black market, mitigation damages like credit monitoring costs are both reasonable and necessary, and not merely "speculative." In an analogous data breach decision, *Anderson v. Hannaford Brothers Co*., the First Circuit held that these damages are recoverable through negligence. 659 F.3d 151, 164 (1st Cir. 2011).

Target's conclusory attack on causation should also be rejected. There is no question that Plaintiffs' allegations that their injuries were the direct result of Target's failure to take necessary precautions to prevent the data breach, as well as its failure to stop the ongoing data breach along any one of the "kill chain" steps, are sufficient to plead causation. The Senate Report supports that conclusion. ¶ 187. Had Target maintained reasonably adequate data security, Plaintiffs never would have suffered damages. And had Target timely notified the public of the ongoing breach, many consumers would not have made payment card purchases at Target and suffered unauthorized (including unreimbursed) charges on their payment cards and unreimbursed fees, overpaid for goods, and incurred the costs of purchasing products they otherwise would not have purchased.

C. The Economic Loss Rule Does Not Apply.

Target errantly contends that in 20 of the jurisdictions at issue, the economic loss rule bars recovery of purely economic losses under a negligence theory. Case law from

around the country uniformly holds that the economic loss rule does not apply to the breach of an independent duty that does not arise from commercial expectations, which Plaintiffs allege. *See* ¶¶ 288-303, 306-310; Pls.' App., Ex. C. *See Grynberg v. Questar Pipeline Co*., 70 P.3d 1, 11 (Utah 2003) ("[T]he modern focus is not on the harm that occurs but instead is on the source of the duty that was breached."). As discussed above, Target's independent duties to reasonably protect Plaintiffs' personal information and to timely notify them of the breach arise from the common law duty of reasonable care, from Minn. Stat § 325E.64, and by virtue of the "special relationship" between the parties.

The principles underlying the economic loss rule include "(1) to maintain the fundamental distinction between tort law and contract law; (2) protect commercial parties' freedom to allocate economic risk by contract; and (3) to encourage the party best situated to assess the risk [of] economic loss, the commercial purchaser, to assume, allocate, or insure against that risk." *KB Home Ind., Inc. v. Rockville TBD Corp*., 928 N.E.2d 297, 303-304 (Ind. Ct. App. 2010) (citations omitted). None of these principles is implicated in a situation where, as here, a plaintiff sues a defendant for breaching an independent duty.

The decisions that Target cites are either wrongly decided outliers or factually distinguishable. In *Willingham v. Global Payments, Inc*., for instance, the plaintiffs sought to recover their losses not from the merchant they shopped at, but from the merchant's payment processor. No. 1:12-CV-01157, 2013WL 440702, at *2 (N.D. Ga. Feb. 5, 2013). The well-settled law in Georgia (as in other jurisdictions) is that "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." *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) (citation and internal quotation marks omitted).

In *Sovereign Bank v. BJ's Wholesale Club, Inc.*, the plaintiff was a credit card issuer and member of the VISA network that sued merchants for failing to take proper precautionary measures to safeguard consumers' financial information, which was exposed in a data breach. 533 F.3d 162 (3d Cir. 2008). Because the VISA operating agreement governed the exact conduct at issue, the economic loss rule applied. *See also Freedom Props., L.P. v. Lansdale Warehouse Co.*, No. 06-5469, 2007 WL 2254422, at *6 (E.D. Pa. Aug. 2, 2007) ("[T]he economic loss doctrine is not a bar when two parties have a special relationship such that a negligent party can foresee harm to the plaintiff.").

In *Sony*, the court misapplied the economic loss rule by holding that because the "duty to provide reasonable network security" was an independent legal duty, the contract between the parties did not bar a parallel tort claim by the plaintiffs unless barred by the economic loss doctrine. *Sony*, 996 F. Supp. 2d at 968. Of course, however, the purpose of finding that an independent tort duty exists is to exclude the claim from the economic loss rule. *Sony* thus conflicts with well-settled law in California that "[t]he economic loss rule requires [a] purchaser to recover in contract for purely economic loss . . . unless he can demonstrate . . . injury arising from a breach of duty which is

independent of the contract[.]" *Frye v. Wine Library, Inc.*, No. 06-5399 SC, 2006 WL 3500605, at *2 (N.D. Cal. Dec. 4, 2006) (citation omitted).

In re Michaels Stores Pin Pad Litigation recognized that in Illinois "the economic loss rule does not apply if the defendant breached a duty owed to the plaintiff independent of any contract." 830 F. Supp. 2d at 530 n.5 (citing *Congregation of the Passion v. Touche Ross & Co.*, 636 N.E.2d 503, 515 (Ill. 1994)). The court simply disagreed with that reading of *Congregation*. Since *Michaels*, courts have continued to interpret *Congregation* as allowing purely economic recovery from the breach of a duty independent of contract. *See, e.g. Rasgaitis v. Waterstone Fin. Group, Inc.*, 985 N.E.2d 621, 637 (Ill. App. Ct. 2d Dist. 2013); *Gondeck v. A Clear Title & Escrow Exch., LLC*, No. 11 C 6341, 2014WL 2581173, at *12 (N.D. Ill. June 9, 2014). *Michaels* is contrary to Illinois law.

VIII. PLAINTIFFS PLAUSIBLY ALLEGE A VALID CLAIM FOR TARGET'S BREACH OF IMPLIED CONTRACT.

As shown in both Target's and Plaintiffs' charts, the basic elements of an implied contract claim are uniform across jurisdictions. *See* Pls.' App., Ex. D; Def.'s App., Ex. D. Plaintiffs plead all of these elements.

Target solicited Plaintiffs to purchase products using their payment cards and Plaintiffs accepted. ¶ 314. Implied in the contract was Target's obligation to safeguard Plaintiffs' private information and to timely and accurately notify them of any breach. ¶ 315. Plaintiffs would not have entrusted their information to Target in the absence of this implied contract. ¶ 316. Plaintiffs fully performed their obligations under the implied

contract. ¶ 317. Target breached the implied contract by failing to safeguard the information and to provide timely and accurate notice that their information was compromised. ¶ 318. Plaintiffs suffered losses as a result of Target's breaches of the implied contract. ¶ 319.

Courts have upheld breach of implied contract claims in data breach cases. In one involving similar facts, the First Circuit reversed the dismissal of the plaintiffs' implied contract claim, explaining that under Maine law, a "contract includes not only the promises set forth in express words, but, in addition, all such implied provisions as are indispensable to effectuate the intention of the parties and as arise from the language of the contract and the circumstances under which it is made." *Anderson v. Hannaford Bros. Co.*, 659 F.3d at 158-59 (citation omitted). Noting that "[t]he existence of such an implied contract is determined by the jury," the court reasoned:

> "When a customer uses a credit card in a commercial transaction, she intends to provide that data to the merchant only. Ordinarily, a customer does not expect – and certainly does not intend – the merchant to allow unauthorized third-parties to access that data. A jury could reasonably conclude, therefore, that an implicit agreement to safeguard the data is necessary to effectuate the contract."

Id. at 159.

Similarly, in *In re Michaels Stores Pin Pad Litigation*, the district court denied the defendant's motion to dismiss the plaintiffs' implied contract claim because the facts evidenced the parties' intent to create "an implicit contractual relationship between Plaintiffs and Michaels, which obligated Michaels to take reasonable measures to protect Plaintiffs' financial information and notify Plaintiffs of a security breach within a reasonable amount of time." 830 F. Supp. 2d at 531.

Target contends that it did not objectively manifest an intention to enter into the implied contract and that Plaintiffs describe only "their unilateral understanding." Def.'s Mem. at 30-33. Essentially, Target maintains it never intended to safeguard consumers' data entrusted to it. But Target has repeatedly and objectively manifested its intention to safeguard customer data. ¶ 233. For years, its privacy policy has publicly stated that it protects customers' personal information. ¶ 234. For example, a May 8, 2006 posting of the policy stated:

> **Our Commitment to Data Security**
> We have appropriate physical, electronics and procedural security safeguards to protect and secure the information we collect.
> **Safe Shopping Guarantee**
> Our security measures are designed to prevent anyone from stealing and using your credit card number.

¶ 234. The version appearing on Target's website on October 3, 2013 and November 7, 2013, stated:

> **How is Your Personal Information Protected?**
> **Security Methods**
> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as credit or debit card numbers, we use industry standard methods to protect that information.

¶ 235.[38] Clearly, the Complaint alleges that Target has objectively manifested an intent and obligation to safeguard customer data.

---

[38] Target concedes that its privacy policy states that it "use[s] industry standard methods to protect" consumer's personal information but that its recent privacy policy language also indicates that no system is completely secure against hackers. Def.'s Mem. at 32. This argument attacks a straw man. Plaintiffs do not contend that Target's systems

Target's denial of the existence of the implied contract simply raises a factual dispute and does not support dismissal of the claim. *See HomeStar Property Solutions, LLC*, 2013 WL 5787667, at *4. Additionally, as the First Circuit noted in *Hannaford*, the existence of an implied contract is a jury determination. *Hannaford*, 659 F.3d at 159. *See also Roberge v. Cambridge Coop. Creamery Co.*, 79 N.W.2d 142, 146 (Minn. 1956) (noting that "[t]he question of whether there is a contract to be implied in fact usually is to be determined by the trier of facts as an inference of fact to be drawn from the conduct of the parties").

Among the circumstances to consider in determining the parties' objective manifestations of intent are Target's legal obligations imposed by law. As mentioned above, Minn. Stat. § 325E.64 prohibits Target from retaining Plaintiffs' card security code data, including the contents of card magnetic stripe data, after authorization of the transaction or, in the case of a PIN debit transaction, longer than 48 hours after authorization of the transaction.

The cases Target relies on support no other conclusion. In *In re Zappos.com, Inc.*, 2013 WL 4830497, at *3, "there is no allegation of any express or implied contract." In *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010), the plaintiffs based their implied contract claim on a brochure given to Starbucks employees and webpage statements, and the court rejected their implied contract claim in the absence of evidence

---

had to be perfect. *See, e.g.*, *Sony*, 996 F. Supp. 2d at 995 (rejecting defendant's argument it disclaimed perfect security).

that plaintiffs had read and relied upon the documents they invoked. Here, Plaintiffs are not relying upon brochures or specific documents but on all of the circumstances surrounding their purchases from Target, including the parties' conduct and mutual objective manifestations of intent.[39] As to Target's contention that Plaintiffs' implied contract claim requires allegations of actual monetary harm, Plaintiffs respectfully refer the Court to their standing discussion in Part IV.

IX. PLAINTIFFS ADEQUATELY PLEAD TARGET'S BREACH OF ITS REDCARD DEBIT CARD AGREEMENTS.

Plaintiffs plead and factually support all elements of a breach of contract claim on behalf of a proposed nationwide class of REDcard Debit Card holders subject to the Target Debit Card Agreement. ¶ 322. The agreement incorporates the Target Debit Card Privacy Policy (¶¶ 322-23), which provides:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. Those measures include computer safeguards and secured files and buildings.

¶ 324.

Plaintiffs allege that, in violation of this provision, their Target REDcard debit cards were compromised in the breach and that they suffered damages and losses detailed

[39] Target argues that an implied contract theory is unavailable to Plaintiffs in Alaska and Pennsylvania because of the existence of an express contract governing the Target REDcards they used. This argument misconstrues the Complaint, which alleges separate counts on behalf of REDcard holders for breach of Target's REDcard agreements (Count V), independent of the breach of implied contract asserted on behalf of all other Plaintiffs in the statewide breach of implied contract classes (Count IV).

above as a direct and proximate result of Target's breach of contract. ¶¶ 329-330.

Focusing on the language of the contract obligating Target to "use security measures that comply with federal law," Target argues that Plaintiffs fail to state a claim because they do not allege a violation of federal law. But to state a contract claim Plaintiffs have no obligation to plead a violation of federal law, which is a legal conclusion; rather, they are obligated to plead facts. Plaintiffs have done just that. As detailed above, the Complaint alleges a wealth of facts showing that Target's woefully deficient "computer safeguards" failed to provide the expressly promised "secured files."

Target's argument that Plaintiffs do not allege damages caused by the breach again disregards their detailed allegations of causation and ten categories of damages. *See* ¶¶ 2.a.-j., 261, 320, 329-330.

X. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM FOR BAILMENT.

A bailment is "the contract or legal relation which is constituted by the delivery of goods without a transference of ownership, on an agreement, expressed or implied, that they be returned or accounted for." *Dennis v. Coleman's Parking & Greasing Stations*, 2 N.W.2d 33, 34-35 (Minn. 1942) (citation omitted). As Target acknowledges, these elements are consistent nationwide. *See* Def.'s Mem. at 37; Def.'s App., Exhibit E.

A. The Modern Definition of Intangible Personal Property Includes Plaintiffs' Payment Card Data.

Courts commonly hold that intangible personal property subject to a bailment includes electronic data. *See Bridge Tower Dental, P.A. v. Meridian Computer Ctr., Inc.*, 272 P.3d 541, 546 (Idaho 2012) (computer hard drive data); *Shmueli v. Corcoran Group*,

802 N.Y.S.2d 871, 877-78 (N.Y. Sup. Ct. 2005) (information stored electronically on a computer); *David Barr Relators, Inc. v. Sadei*, No. 03-97-00138-CV, 1998 WL 333954, at *3 (Tex. App. Austin June 25, 1998) (computer data). Courts have treated payment card data the same way in applying the related but separate common law tort of conversion. *Welco Elecs., Inc. v. Mora*, 166 Cal. Rptr. 3d 877, 884 (Cal. Ct. App. 2014) ("Plaintiff had a property right in its credit card account because plaintiff[']s interest was specific, control over its credit card account, and an exclusive claim to the balance."); *In re Easysaver Rewards Litig.*,737 F. Supp. 2d 1159, 1180 (S.D. Cal. 2010) ("[T]he Court concludes that Plaintiffs may state a conversion claim based upon the misappropriation of their Private Payment Information, which was then used to make allegedly unauthorized debits from their financial accounts. Possession of the debit card or PayPal account information is similar to the intangible property interest in a check.").

Target's assertion that a merchant must take exclusive possession and control over payment card data is wholly at odds with the growing body of case law recognizing the need to expand the definition of intangible personal property and minimize or eliminate any exclusivity requirement under state law. *See Bridge Tower Dental*, 272 P.3d 541, 546 (computer hard drive data); *Shmueli*, 802 N.Y.S.2d 871, 877-78 (bailment of computerized proprietary information); *David Barr Relators*, 1998 WL 333954, at *3 (computer data). *See also Afremov v. Amplatz*, No. A09-1157, 2010 WL 2035732, at *6 (Minn. Ct. App. May 25, 2010) (electronic litigation data copied from its original source).

Target's reliance on *Beech Transportation v. Critical Care Services*, No. C6-01-292, 2001 WL 1182707 (Minn. Ct. App. Oct. 9, 2001), is misplaced. *Beech* involved the

alleged bailment of an airplane, not intangible property. *Id*. at *3. In addition, there was no direct relationship between the parties and the plaintiff retained certain rights to control the airplane while in the defendant's possession. *Id*. Here, Plaintiffs and Target *did* have a direct relationship and Plaintiffs *did not* retain any right to control how Target stored their personal information.[40]

B. The Parties Understood and Expected That Target Would Dispose of Plaintiffs' Payment Card Data Upon Completion of the Sale in Compliance with Legal and Industry Requirements.

Plaintiffs sufficiently allege that the parties had an implied agreement that following the purchase transaction Target would account for Plaintiffs' financial information in compliance with legal requirements and industry standards. *See* ¶¶ 195, 197, 312-319, 339. As discussed above, they allege that Minnesota law prohibits Target from retaining payment card data more than 48 hours after authorization of the transaction." ¶ 195. Industry standards also prohibit Target from retaining certain

---

[40] Target also cites *Sony I*, 903 F. Supp. 2d 942, 974 and *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008). Neither of these decisions considered either *Easysaver Rewards Litigation*,737 F. Supp. 2d 1159 or *Welco Electronics, Inc. v. Mora*, 166 Cal. Rptr. 3d 877, which both acknowledge that California law has greatly expanded the tort of conversion "well beyond its original boundaries" to include intangible personal property. *Welco*, 166 Cal. Rptr. at 883.

Sony I misapplied the law by requiring an allegation that the defendant engaged in conversion or other intentional conduct. Bailment *does not* require that a defendant engaged in any intentional conduct; it may arise under a negligence theory. *E.g.*, *Leighton v. Rossow*, No. A09-776, 2010 WL 772341, at *5 (Minn. Ct. App. Mar. 9, 2010) ("[A] duty of due care arises in a bailment relationship, and damage to the bailee's property is therefore addressed under a negligence theory, and not merely as a breach of the bailment contract.").

customer data. ¶ 197. As the Complaint alleges, "Target failed to return, purge or delete the personal and financial information of Plaintiffs and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law." ¶ 339.

XI. THE COURT SHOULD DENY TARGET'S MOTION TO DISMISS PLAINTIFFS' UNJUST ENRICHMENT CLAIMS.

A. Plaintiffs Have Alleged Plausible Unjust Enrichment Claims.

"Unjust enrichment occurs when a person retains a benefit (usually money) which in justice and equity belongs to another." *Movahedi v. U.S. Bank, N.A.*, 853 F. Supp. 2d 19, 29 (D.D.C. 2012) (citations omitted). The essential elements of unjust enrichment are common across jurisdictions. *See* Pls.' App., Ex. E. "[A] plaintiff states a claim for unjust enrichment when: (1) the plaintiff confers a benefit upon the defendant; (2) the defendant retains the benefit; and (3) under the circumstances, the defendant's retention of the benefit is unjust." *Saber Int'l Sec. v. Torres Advanced Enter. Solutions, Inc.*, 820 F. Supp. 2d 62, 76 (D.D.C. 2011) (citations omitted). Damages for unjust enrichment are "based on what the person allegedly has received, not on what the opposing party has lost." *Georgopolis v. George*, 54 N.W.2d 137, 142 (Minn. 1952).

The first two unjust enrichment elements are clearly satisfied. As to the third, Plaintiffs allege they would not have shopped at Target during the data breach had Target made proper disclosures. ¶¶ 343-344, 348. Plaintiffs paid for goods purchased at Target stores with money that was supposed to be used by Target, in part, to provide for adequate data security. ¶¶ 345-346. Target should return the money it unjustly received for protection it failed to provide.

Target argues that Plaintiffs have not alleged facts showing that they overpaid for the products they purchased from Target. Def.'s Mem. at 38-39 (citing *Zappos*, 2013 WL 4830497, at *5).[41] *Zappos* does not support this argument. Plaintiffs in that case did not allege that a portion of their payment was intended to go towards data security. Furthermore, Target completely ignores *Resnick v. AvMed, Inc*., where the Eleventh Circuit reversed the district court's dismissal of virtually identical allegations. 693 F.3d 1317, 1328 (11th Cir. 2012). The plaintiffs there sued their health insurance provider after thieves stole two laptop computers containing the plaintiffs' unencrypted personal information. *Id.* at 1322. Like here, the plaintiffs alleged that part of their monthly insurance premiums "were intended to pay for the administrative costs of data security[,]" and because the defendant did not properly secure the plaintiffs' data, it would be inequitable for the defendant to retain their premiums. *Id.* at 1328. The defendant made the same argument that Target raises here: "Plaintiffs paid [the defendant] not for data security but for health insurance." *Id*. Reversing the lower court's dismissal of this claim, the Eleventh Circuit found that the plaintiffs had alleged sufficient facts to survive a motion to dismiss. *Id.*

The cases Target cites do not support its argument that the Court should reject Plaintiffs' allegation that they would not have purchased products at Target stores had Target disclosed its inadequate data security or the breach. All can be distinguished on

[41]To the extent that Target relies on its arguments regarding Article III standing in support of its arguments regarding Plaintiffs' unjust enrichment claims, Plaintiffs address those arguments in Part IV.

their facts. In *In re Sony PS3 "Other OS" Litigation*, for example, the court dismissed an unjust enrichment claim where, unlike here, the plaintiffs failed to "allege[] sufficient facts as to the terms and conditions on which they paid monies to [the defendant]." 551 F. App'x 916, 923 (9th Cir. 2014). In *Hughs v. Chattem, Inc.*, unlike here, the plaintiff "fail[ed] to allege extraordinary circumstances" that made the defendant's enrichment unjust. 818 F. Supp. 2d 1112, 1124-25 (S.D. Ind. 2011). The facts of Target's misconduct alleged by Plaintiffs constitute extraordinary circumstances by any measure. *See supra*, at 2-4. None of the decisions Target cites reject Plaintiffs' theory that Target was unjustly enriched with consumers' money that it would not have received, but for its misconduct.

B. California Would Recognize Unjust Enrichment As an Independent Cause of Action.

Target incorrectly argues that California does not recognize unjust enrichment as an independent cause of action. As recognized in *Sony I*, to which Target cites, there are conflicting rulings on whether California recognizes the claim. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 973-74 (S.D. Cal. 2012). The better reasoned view, consonant with the law prevailing in other states, recognizes the claim. *See Berger v. Home Depot USA, Inc.*, 741 F.3d 1061, 1070 (9th Cir. 2014) (recognizing unjust enrichment as an independent claim); *Imber-Gluck v. Google, Inc.*, No. 5:14-CV-01070, 2014 WL 3600506, at *7-8 (N.D. Cal. July 21, 2014) (same); *In re Processed Egg Prods. Antitrust Litig.*, 851 F. Supp. 2d 867, 913 (E.D. Pa. 2012) (declining to dismiss California unjust enrichment claims because "California courts have

not uniformly or definitively barred an independent cause of action for unjust enrichment").

C. Plaintiffs in Alaska and Pennsylvania May Plead Their Unjust Enrichment Claims in the Alternative.

When the unjust enrichment recovery sought is not clearly covered by contract, it is improper to dismiss an unjust enrichment claim at the pleading stage. *Ellis v. J.P. Morgan Chase & Co*., 950 F. Supp. 2d 1062, 1090-91 (N.D. Cal. 2013) ("Despite Defendants' arguments that the mortgage agreements preclude the claim here, the Court finds it is premature for the Court to take a position on whether this action derives from the subject matter of the agreements such that a claim for unjust enrichment is unavailable."); *In re Countrywide Fin. Corp. Mortg. Mktg. & Sales Practices. Litig*., 601 F. Supp. 2d 1201, 1220-21 (S.D. Cal. 2009) ("Although there are contracts at issue in this case, none appears to provide for the specific recovery sought by Plaintiffs' unjust enrichment claim.").

Plaintiffs are entitled to plead their claims in the alternative under Rule 8(a)(2). *See, e.g., Progressive N. Ins. Co. v. Alivio Chiropractic Clinic, Inc*., No. 05-0951, 2005 WL 3526581, at *4 (D. Minn. Dec. 22, 2005) (Magnuson, J.) (denying motion to dismiss unjust enrichment claim pled in the alternative to a breach of contract claim and observing that "Federal Rule of Civil Procedure 8 permits pleading claims in the alternative, and dismissal is not warranted on this basis"); *Blennis v. Hewlett-Packard Co*., No. 07-00333, 2008 WL 818526, at *4 (N.D. Cal. Mar. 25, 2008) (holding that plaintiffs had right to plead quasi-contract/unjust enrichment theory in alternative, even

though it was duplicative of express contract claim); *Infowise Solutions, Inc. v. Microstrategy Inc*., No. 3:04-CV-0553-N, 2005 WL 2445436, at *7 (N.D. Tex. Sept. 29, 2005) ("A plaintiff may demand relief under alternative theories. . . . This allows a plaintiff to plead both breach of contract or unjust enrichment claims.").

The legal authority on which Target relies is inapposite. In *Nicdao v. Chase Home Finance*, the court dismissed claims after a judgment on the pleadings, not on a motion to dismiss. 839 F. Supp. 2d 1051, 1061 (D. Alaska 2012). And in *Seifert v. Prudential Insurance Co. of America*, Judge Slomsky dismissed an unjust enrichment claim because it arose from a contractual provision which the court held had not been breached. No. 13-7637, 2014 WL 2766546, at *7 (E.D. Pa. June 18, 2014). More apposite is *Coleman v. Commonwealth Land Title Insurance Co*., where Judge Slomsky allowed an unjust enrichment claim to be pled in the alternative. 684 F. Supp. 2d 595, 621 (E.D. Pa. 2010) (quoting *Sudofsky v. JDC, Inc*., No. 03-1491, 2003 WL 22358448, at *4 (E.D. Pa. Sept. 9, 2003) ("Plaintiff's claims are alternative theories of recovery based on the same factual circumstances. It would serve no purpose at this early point in the litigation to limit Plaintiff's avenues of recovery when the underlying facts and events for all claims are the same.")).

XII. CONCLUSION

Target has not met its heavy burden under Rule 12(b)(6). Its motion to dismiss should be denied in its entirety.

Date: October 31, 2014

s/ *Vincent J. Esades*
Vincent J. Esades (249361)
David Woodward (018844X)

HEINS MILLS & OLSON, P.L.C.
310 Clifton Avenue
Minneapolis, MN 55403
Tel.: (612) 338-4605
Fax: (612) 338-4692
vesades@heinsmills.com
dwoodward@heinsmills.com

Lead Counsel Consumer Cases

E. Michelle Drake (0387366)
NICHOLS KASTER, PLLP
4600 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel.: (612) 256-3200
Fax: (612) 338-4878
drake@nka.com

Liaison Counsel Consumer Cases

John A. Yanchunis
MORGAN & MORGAN COMPLEX
LITIGATION GROUP, PA
201 North Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
Fax: (813)-223-5402
jyanchunis@forthepeople.com

Executive Committee - Coordinating Lead and Liaison Counsel

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

Ariana J. Tadler
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, NY 10119
Tel.: (212) 594-5300
Fax: (212) 868-1229
atadler@milberg.com

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel.: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com

Steering Committee Consumer Cases