UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Financial Institutions Cases	MDL No. 14-2522 (PAM/JJK) **FINANCIAL INSTITUTION PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANT TARGET CORPORATION'S MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT**
Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain, Individually and on behalf of a class of all similarly situated financial institutions in the United States, Plaintiffs, v. Target Corporation, Defendant.	JURY TRIAL DEMANDED

TABLE OF CONTENTS

Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain (collectively, "Plaintiffs"), individually and on behalf of a class of similarly situated financial institutions, hereby respond to Defendant Target Corporation's ("Target," "Company" or "Defendant") Motion to Dismiss the Consolidated Class Action Complaint ("Target Br.") (ECF No. 185).[1]

I. INTRODUCTION

According to Target, it has no liability whatsoever for the 2013 data breach (the "Breach"), regardless of its culpability. Target says it owes nothing to its retail customers, asserting that those plaintiffs lack standing to sue because they are not the ones who lost money due to the Breach. *See* ECF No. 35 at 5-7. As for the financial institutions that, at a minimum, have spent tens of millions of dollars canceling and issuing new cards, Target claims it owes them no duty of care and has not violated Minnesota's card data security law. In Target's view, it can reap 100% of the benefits of non-cash transactions, and bear 0% of the risks of exposure that necessarily accompany such transactions, even if its security is grossly deficient. *See* Target Br. at 6 (asserting no duty to anyone, even if Target knew that "action on [its] part was *necessary* for [financial institutions'] aid or protection."). Target is wrong.

The Breach, which compromised the records of 110 million customers and caused Plaintiffs enormous losses, would not have happened if Target's defective data security

[1] Throughout this brief, citations to paragraphs in the Consolidated Class Action Complaint ("Complaint") (ECF No. 163) appear as "¶__," and all emphasis is added and internal citations or quotations omitted unless otherwise stated.

practices had not let it happen. Target's failures that enabled the Breach are a matter of public record, having been aired in hearings before a United States Senate Committee and analyzed in reports of investigative journalists and technology experts. Among its multiple failures, Target: (1) voluntarily disabled security functions that would have automatically deleted the "malware" that carried out the Breach; (2) ignored urgent alerts from its computer security programs about the malware's presence on, and exfiltration of data from, Target servers; (3) improperly retained card data for months after card transactions and did not segregate sensitive data in its network; (4) ignored pre-Breach warnings from its employees about its computer system's obvious vulnerabilities to cyber-attack; and (5) declined to implement critical security measures pursuant to industry warnings and standards, any of which could have prevented the Breach. Target's deficient conduct violated standards applicable to it under the Minnesota Plastic Card Security Act, Minn. Stat. § 325.64 ("PCSA" or "Act") and common law.

Notwithstanding the public facts establishing that ***Target*** ignored warnings and turned off detection programs, Target argues that it is not liable for Plaintiffs' losses flowing from the Breach. Target argues that it did not violate the PCSA – the Minnesota Legislature's response to card data thefts precisely like the Breach – because it did not retain card data as prohibited by the Act. Target Br. at 26-29. This argument contradicts Plaintiffs' allegations that Target retained card data through its corporate data storage practices and its decision not to delete neither the malware to which it was alerted nor stolen card data on its servers during the Breach. *See infra* Section IV.A. Target's

argument contesting Plaintiffs' negligence *per se* claim fails alongside Target's PCSA argument because it rests entirely on the purported failure of Plaintiffs' PCSA claim.

Target also asserts that it owed no duty to Plaintiffs to safeguard card data. Target Br. at 5-14. Relevant case law states otherwise. Numerous courts in other data breach cases, applying general negligence principles, have recognized that businesses that undertake card transactions have a duty to card-issuing banks like Plaintiffs to responsibly secure card data. *See infra* Sections IV.C.1-3, IV.D. Minnesota's analysis regarding general negligence duty (which Target ignores) overwhelmingly confirms Target's duty to Plaintiffs, and alternatively, Target's duty under Minnesota's special relationship standard is also clear. Moreover, the PCSA conclusively negates Target's argument that Plaintiffs are unforeseen victims or that Target is not responsible for the acts of hackers.

Lastly, Target argues that Plaintiffs have not properly alleged negligent misrepresentation by omission because Target was not obligated to make accurate representations, Target omitted nothing, and Plaintiffs have not pled reliance. Target Br. at 16-25. The first two arguments fail because they mischaracterize Plaintiffs' allegations, while the last argument fails because reliance on an omission need not be pleaded. *See infra* Section IV.D.

Each of Plaintiffs' claims is well-pleaded. Defendants' motion should be denied.

II. STATEMENT OF FACTS

This case seeks recovery on behalf a class of financial institutions who were forced to absorb millions of dollars in costs because of Target's negligence and statutory

violations, which resulted in the release of sensitive financial data of approximately 110 million Target shoppers in the Breach – one of the largest data compromises in the history of the United States. ¶1. Criminal hackers are a given in data breaches, but merchants like Target are obligated by industry standards and Minnesota law to take certain steps to ensure that sensitive financial data is not compromised.

Target Was Obligated to Protect Card Data.

In addition to common law duties requiring Target to act reasonably to safeguard confidential card data, the Company is obligated to protect its customers' data pursuant to specific standards including:

- Payment Card Industry Data Security Standards ("PCI DSS"), which require merchants to, *inter alia*, protect cardholder data, ensure maintenance of vulnerability management programs and information security policies, implement strong access control measures, and regularly monitor and test networks;

- Card Operating Regulations issued by credit and debit card companies, which require merchants to maintain the security and confidentiality of cardholder information; and

- The PCSA, which regulates a merchant's storage/deletion of card data and states that no merchant "shall retain" certain card data after the authorization of a credit card transaction (or 48 hours after a debit card transaction). The Act provides for statutory damages but specifically states that the remedies it provides supplement other remedies.

¶¶17-20. Target blatantly disregarded these standards.

Among other things, Target, in violation of the PCI DSS and PCSA, maintained a general practice of retaining customer card data, including full account numbers, expiration dates, cardholder names and CVV security codes (a 3-4 digit value printed on

credit and debit cards) for 60 to 80 days. ¶¶80-82. Target's corporate policy of retaining data was all the more questionable in light of its prior computer security issues, including breaches in 2005 and 2010. *See* ¶¶26-27.

Notwithstanding Target's retention of payment data, it also purportedly took steps to strengthen certain elements of its system's defenses. Target hired FireEye, a renowned security software company, to update Target's computer security. ¶34. FireEye's software included state-of-the-art malware detection, and, important to the Breach, an automatic malware deletion function. This function could have prevented the Breach, but Target inexplicably turned it off, paving the way for an incursion. ¶77.

Target Ignored Specific Warnings Before and During the Breach.

Before the Breach occurred, Target received multiple warnings of cyber-attacks employing RAM-scraper programs. ¶¶30-31. In April and August 2013, Visa issued reports alerting Target about potential attacks using RAM-scraper malware to extract full magnetic stripe data – the type of malware used and data extracted in the Breach. *Id*. These warnings provided Target with specific measures to combat such breaches, however Target did not implement any of the measures. ¶32. In September 2013, Target's own security staff raised concerns about vulnerabilities in Target's payment system. These reports and warnings went unheeded. ¶43.

The hackers orchestrating the Breach obtained access to Target's system through a third-party vendor, "Fazio," that had access to Target's network, but who was not required by Target to maintain adequate computer security. ¶¶37-38, 41. On November 15, 2013, the hackers uploaded card-stealing malware onto Target's computer network

(the malware reached most in-store cash registers by November 30). ¶¶45-49. Hackers also installed exfiltration malware, designed to store data on Target's own system, then move it after several days, to the hackers' system. ¶56. The hackers' activities did not go undetected. On November 30, FireEye identified the malware and notified Target of its presence. ¶53. Target did nothing in response. ¶¶50, 53, 54. Separately, Target's antivirus system identified similar activity and warned Target. Again, Target took no action. ¶53. On December 2, FireEye again notified Target about the malware. ¶54. Target did not respond. *Id.*[2]

Once inside Target's system, the hackers began collecting card data. ¶¶55-57. From December 2-15, card data was collected as it was swiped at Target stores. *Id.* The card data was stored on Target's system for six days, after which the malware sent it to a server in Russia. *Id.* Target allowed this collection and storage to occur for almost two weeks, despite it having been detected and having opportunities to cut it short. ¶¶55-57. Beyond the prior alerts, on December 11, a Target employee observed and reported the malware, but Target did nothing, and the Breach continued. ¶60. On December 12, the Department of Justice alerted Target about the Breach, but Target, showing no urgency to respond, did not begin purging its system of the malware until December 15, three days later. ¶¶65-66. Target finally publicly acknowledged the Breach on December 19, a week after being notified by federal authorities. ¶68. During this time and throughout

[2] Aside from responding to the numerous warnings, Target could have prevented the Breach by: segmenting its system, requiring two-factor authentication, eliminating unneeded default accounts, requiring vendors to monitor the integrity of their files, erecting strong firewalls, and only allowing its network to upload to approved servers. ¶¶47-48, 52, 58-59.

the month of December, financial institutions' card data was being sold on the black market. ¶¶61-62.

All told, the Breach affected approximately 110 million people, including customers who had not swiped cards during the Breach, meaning that information stored through Target's general practice of retaining customers' card data for 60-80 days was compromised. ¶¶71-75, 82. The Breach caused Plaintiffs to expend considerable resources and resulted in physical damage to Plaintiffs' property. Plaintiffs, among other things, were forced to reissue cards, change or close accounts, notify customers about the Breach, investigate claims of fraud, refund customers for fraudulent charges and increase fraud monitoring. ¶¶85-86.

After the Breach, an investigation by the Senate Committee on Commerce, Science and Transportation commenced. ¶¶51-52, 78. It revealed that Target had missed multiple opportunities to prevent the Breach, including alerts received from FireEye on November 30 and December 2 that were impossible to miss and early enough that the Breach could have been stopped before any data was stolen. *Id.* A *Bloomberg* investigation additionally confirmed that FireEye had installed a function that automatically deleted malware, which Target had disabled before the Breach. ¶77. *The New York Times* reported that Target's computer system was "astonishingly" open and "particularly vulnerable to attack." ¶79. Target itself has stated that it expects a forensic investigator to find that Target was not in compliance with PCI-DSS at the time of Breach. ¶44.

III. LEGAL STANDARD

In evaluating a motion under Rule 12(b)(6), "a court assumes all facts in the complaint to be true and construes all reasonable inferences from those facts in the light most favorable to the complainant." *United States ex rel. Raynor v. Nat'l Rural Utils. Coop. Fin., Corp.*, 690 F.3d 951, 955 (8th Cir. 2012). To survive dismissal, a complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 547 (2007). Although a complaint need not contain "detailed factual allegations," it must provide enough specificity "to raise a right to relief above the speculative level." *Id.* at 555. A claim is plausible when the 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). "[T]he 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).

Here, the Complaint plausibly pleads claims for a violation of the PCSA, negligence *per se*, negligence and negligent misrepresentation by omission through particularized factual allegations that satisfy the applicable pleading standards. There is no basis to dismiss any Count of the Complaint.

IV. ARGUMENT

A. Plaintiffs Have Adequately Pled a Claim Under the Plastic Card Security Act.

The Minnesota Legislature specifically enacted the PCSA to compensate financial institutions for losses suffered from data breaches like the one at issue here. ¶¶20-21, 25, and n.1. Despite the Act's unambiguous language and clear application to this case, Target argues that it cannot be held accountable because – contrary to Plaintiffs' allegations that Target retained card data in violation of the Act, *see* ¶¶50-51, 53-60, 66, 71-75, 77-78, 80-83 – Target claims that it did not retain such data. *See* Target Br. at 26-29. Target's argument ignores Plaintiffs' factual allegations and asks the Court, improperly, to adopt its version of events at this stage. *See Country Inns & Suites by Carlson, Inc. v. Praestans One, L.L.C.*, No. 13-cv-3381, 2014 WL 3420800, at *9 (D. Minn. July 14, 2014) (denying motions to dismiss while construing alleged facts as true and "in the light most favorable to the plaintiff").

The PCSA strictly prohibits Minnesota businesses like Target from "retaining" specified card information, including "the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data" (hereinafter, "protected card data"), beyond specified time periods: a business violates the Act if it fails to delete protected card data immediately after a credit card transaction is authorized, or within 48 hours after a debit card transaction is authorized. *See* Minn. Stat. § 325E.64, Subd. 2. If a merchant retains protected card data longer than the statute allows and "there is a breach of the security" of that merchant, the Act requires the

merchant to compensate financial institutions "affected by the breach" (like Plaintiffs) for their costs associated with "reasonable actions undertaken as a result of the breach." Minn. Stat. § 325E.64, Subd. 3. Recoveries under the Act include, "***but [are] not limited to***," canceling and issuing new cards, closing and opening accounts and refunding cardholders for unauthorized charges. *Id*. Moreover, the Act expressly preserves common law remedies available to financial institutions against businesses in connection with card data breaches, providing that "the remedies under this subdivision are cumulative and ***do not restrict any other right or remedy otherwise available to the financial institution***." *Id*. Plaintiffs' allegations fit the Act's requirements exactly. *See* ¶¶21, 28, 50-51, 53-60, 66, 71-75, 77-78, 80-83.

1. Target's Business Strategy of Storing Protected Card Data Violated the PCSA.

Plaintiffs allege that Target "retained" protected card data in violation of the Act through a general corporate policy and practice of storing "sensitive customer financial data for 60 to 80 days." ¶82. As alleged, Target stored information from card transactions, including "the account numbers … the expiration date and the cardholder's name," as well as the "CVV codes" (¶75), for two-to-three months after such transactions occurred. ¶¶75, 80-83. This is precisely the type of card information that Target admitted was taken in the Breach. ¶71. The fact that Target stored card data from customer transactions is underscored by the Senate Report, which discusses how the breach affected "***areas of Target's network … storing consumer data***." ¶78. Plaintiffs' allegations in this regard easily satisfy the Rule 8(a) pleading standard.

Target's argument that these allegations are "undercut" by the Complaint's "allegations of how the Intrusion occurred" because "Banks [do not] allege that the particular payment card data referenced in Paragraph 82 was affected by the Intrusion," Target Br. at 29, contradicts the Complaint. *See* ¶¶71, 78, 82. Indeed, Plaintiffs allege that the information referenced in Paragraph 82 was affected by the Breach, for example, through allegations quoting a security expert, who stated, "[t]he fact that three-digit CVV security codes were compromised" in the Breach "shows they were being stored." ¶82; *see also* ¶¶71, 78. The Act bars businesses from retaining CVV codes, as Target did here. *See* Minn. Stat. § 325E.64, Subd. 2 (prohibiting retention of "***card security code*** data. . . ."); *id.*, Subd. 1(d) (defining "Card security code" to include CVV code). Thus, Target stored and retained protected card data. The undisputed fact that this data was later compromised in the Breach establishes Target's liability under the PCSA. *See id.*, Subd. 3; *see also* ¶¶71, 82.

2. Target Retained Protected Card Data on its Servers During the Data Breach for Six Days at a Time.

Plaintiffs also allege that Target retained protected card data in violation of the Act between November 30 and December 15, 2013 by disabling malware-security functions, ignoring repeated alerts as to the ongoing Breach, and otherwise affirmatively electing not to delete malware that warehoused protected card data on its servers for at least six days at a time. ¶¶50-51, 53-60, 65-67, 77-78. Target argues that it did not "retain" the protected card data because hackers put the data on Target's servers. Target Br. at 28-29. This argument ignores the plain language of the PCSA. ¶¶58-60, 65-67, 77-78.

The Act prohibits Minnesota businesses from "retain[ing]" protected card data. Minn. Stat. § 325E.64, Subd. 2. When interpreting statutory text, the Minnesota Supreme Court "give[s] words and phrases their plain and ordinary meaning." *In re Welfare of J.J.P.*, 831 N.W.2d 260, 264 (Minn. 2013) (citing Minn. Stat. § 645.16). The plain and ordinary meaning of "retain" is to "continue to have something." Oxford Dictionary, American English (2014).[3] The Act contains no requirement as to how or in what manner a business retains card data in its control, nor does it include a scienter requirement. *See Energy East Corp. v. U.S.*, 645 F.3d 1358, 1362 (Fed. Cir. 2011) (noting that the "court cannot simply add phrases or words that do not appear in the statute; doing so would be phantom legislative action"); *Goplen v. Olmsted Cnty. Support & Recovery Unit*, 610 N.W.2d 686, 689 (Minn. Ct. App. 2000) ("In interpreting statutes, a court cannot supply that which the legislature purposely omits or inadvertently overlooks"). To the extent Target contends that it did not violate the PCSA because its conduct purportedly did not contribute to the protected card data being stored on Target's computer system, this simply attempts to contradict Plaintiffs' allegations, which detail how (1) Target stored protected card data pursuant to corporate policy (¶¶75, 80-83); and (2) Target had complete discretion to delete the malware and the protected card data on its servers, but instead chose to ignore repeated warnings from its computer security providers and to turn off malware security functions that would have purged the malware and data (¶¶50-60, 77-78). By thus allowing the protected card data to remain on its

[3] http://www.oxforddictionaries.com /us/ definition/american_english/retain (last visited Sept. 29, 2014.)

servers, Target retained the data and violated the Act. The plain language of the Act forbids, without qualification, a business from retaining protected card data beyond the statutory time period.

Here, there is no dispute that Target "continued to have" protected card data ***on its servers*** for more than the allowable period. *See* ¶¶55-60, 66-67, 75, 82. Target's arguments seeking to explain away how this data was stored for days on its servers fly in the face of Plaintiffs' allegations and raise factual issues which cannot be resolved in Target's favor at this stage.

Target also asserts that Plaintiffs have not sufficiently alleged that the "card security code," the "PIN verification code," or the full "magnetic stripe data" were retained. *See* Target Br. at 27. Once again, this argument contradicts the Complaint's allegations. *See Zutz v. Nelson*, 601 F.3d 842, 848 (8th Cir. 2010). In particular, Plaintiffs allege that the "card security code," the "PIN verification code," and the full "magnetic stripe data" were retained on Target's system for periods of six days. ¶¶50, 56-60, 71-75. Further, Plaintiffs allege that Target had a practice of retaining full account numbers, expiration dates, names and CVV codes for longer periods of time. ¶¶75, 80-83. Target's self-serving spin on these allegations cannot support dismissal under Rule 12.

Additionally, the purpose underlying the PCSA's enactment supports imposing liability on Target. Indeed, "the goal of all statutory interpretation is to ascertain and effectuate the intent of the Legislature." *In re Welfare of J.J.P.*, 831 N.W.2d at 264. Here, Plaintiffs have specifically alleged that the PCSA was intended to incentivize

Minnesota businesses to safeguard card data and to protect card-issuing financial institutions from the consequences of poor data security by businesses. *See* ¶¶20-21, 25, 25 n.1. This intent would be thwarted if Target is able to avoid liability under the Act in the circumstances alleged, in which it maintained a policy of storing protected card data and chose not to delete the malware and protected card data on its servers, and thus required card-issuing financial institutions to undertake costly activities in direct response to the Breach. *See* Minn. Stat. § 325E.64, Subd. 3.

Finally, Target does not contest Plaintiffs' allegations addressing the PCSA's other provisions, regarding, *inter alia*, liability, causation and injury. Plaintiffs' allegations concerning these other provisions readily satisfy Rule 8(a):

- Plaintiffs' allegations that while in violation of the Act Target experienced a computer system data breach, *see* ¶¶45-60, 65-67, 71-78, meet the Act's provision creating liability "[w]henever there is a breach of the security of the system of a person or entity that has violated this section," Minn. Stat. § 325E.64, Subd. 3;

- Plaintiffs' causation allegations describing their reasonable prophylactic and remedial actions taken in response to the Breach, *see* ¶¶2, 15-16, 71-77, 85-87, 123, 125, meet the Act's requirement that liability be limited to "costs of reasonable actions undertaken by the financial institution as a result of the breach," Minn. Stat. § 325E.64, Subd. 3; and

- Plaintiffs' damages allegations describing costs from card reissuance and various account-related actions explicitly recognized as reasonable under the Act, *see* ¶¶85-87, 123, satisfy the Act's damages provisions, Minn. Stat. § 325E.64, Subd. 3(1-5).

3. The Act Applies to Card Data Retained by Target.

Target next argues that Plaintiffs' claim under the Act must be limited to protected card data from transactions that occurred in Minnesota. *See* Target Br. at 29-30. This argument distorts the actual language of the PCSA.

By its plain terms, the Act applies to any "person or entity conducting business in Minnesota that accepts an access device in connection with a transaction …" – *i.e.*, Minnesota businesses. *See* Minn. Stat. § 325E.64, Subd. 2. Target attempts to read the statutory terms "conducting business in Minnesota" and "transaction" to limit the Act so that it applies only to card data from transactions in Minnesota. However, the Act does not regulate the actual transactions between businesses and customers (wherever they may occur), but the retention and deletion of protected card data by Minnesota businesses ***after*** such transactions. *Id.* The Act is violated not by anything a business does with card data during a "transaction," but when a business or service provider "retains such data subsequent to the authorization of the transaction" beyond the statutorily permissible time period. *Id.* Moreover, a business is liable under the Act only where it retains protected card data and its computer "system" housing the data is then breached, further undermining Target's attempts to limit the Act's application to ***transactions*** in Minnesota. *See id.*, Subd. 3. Finally, the Act does not define or limit the word "transaction" in any respect, let alone on a geographical basis. Target's argument is flatly incompatible with the Act's plain language. *See In re Welfare of J.J.P.*, 831 N.W.2d at 264 ("[i]n interpreting statutory language, we give words and phrases their plain and ordinary meaning").

4. Target's Dormant Commerce Clause Argument Is Misplaced.

Target's footnoted reference to the dormant Commerce Clause, *see* Target Br. at 30 n.11, also fails. The Minnesota Legislature may clearly regulate the data retention activities of Minnesota businesses such as Target, regardless of where the data originates.

Here, Plaintiffs allege that the Act applies to a Minnesota corporation, headquartered in Minnesota and with its security operations center in Minnesota. ¶¶5-6, 13, 20, 25, 28. The Complaint alleges that Target violated the Act through its card data storage and deletion practices and conduct in November and December 2013. Minnesota has a substantial interest in regulating its corporations and their conduct, which is precisely what the PCSA is alleged to do here. *See Mooney v. Allianz Life Ins. Co. of N. Am.*, 244 F.R.D. 531, 535 (D. Minn. 2007) (rejecting defendant's argument that the "application of Minnesota law to the claims of non-Minnesota class members would offend the Commerce Clause by effectively making Minnesota a national regulator of sales transactions" because "Minnesota has a substantial interest in policing the conduct of its corporations so as to 'prevent[ ] the corporate form from becoming a shield for unfair business dealing.'") (quoting *CTS Corp. v. Dynamics Corp. of Am.*, 481 U.S. 69, 93 (1987)); *Khoday v. Symantec Corp.*, No. 11-cv-180, 2014 WL 1281600, at *20 n.10 (D. Minn. Mar. 13, 2014) (rejecting defendant's argument that dormant Commerce Clause applies to Minnesota consumer protection statute where defendant was Minnesota corporation headquartered in Minnesota and significant conduct violating the statute occurred in Minnesota). Accordingly, Target's dormant Commerce Clause argument is unavailing.

B. Plaintiffs Have Adequately Alleged a Claim for Negligence *Per Se*.

Target tacitly concedes that if Plaintiffs' claim under the PCSA is adequately alleged (as it is), then Plaintiffs' negligence *per se* claim should stand. Indeed, Target's lone argument against Plaintiffs' negligence *per se* claim is that Plaintiffs have failed to

plead the necessary predicate violation of the PCSA. *See* Target Br. at 30. Target does not dispute that Plaintiffs have properly alleged the other elements of the claim – causation and damages.

A "*per se* negligence rule 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 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.) (citing *Gradjelick v. Hance*, 646 N.W.2d 225, 231, n.3 (Minn. 2002)). Because, as noted above, Plaintiffs have plausibly alleged that Target violated the PCSA, they have established the duty and breach elements of their negligence *per se* claim. *See supra* at Section IV.A; *see also* ¶¶ 20-21, 28, 50-51, 53-54, 56-60, 66, 71-75, 77-78, 82-83, 85-86, 95 (alleging that Target had a policy of storing protected card data and failed to purge malware and protected card data that was on its servers for days). Moreover – as Target does not dispute – Plaintiffs sufficiently allege the remaining two elements of negligence *per se*, causation and damages. *See, e.g.*, ¶¶2, 15-16, 71-77, 86, 95, 123, 125 (alleging that Target's card data security failures proximately caused injury to Plaintiffs).

Target offers a single, entirely distinguishable case in support of its negligence *per se* argument. *See* Target Br. at 30 (citing *Yang Mee Thao-Xiong v. Am. Mortg. Corp.*, No. 13-cv-354, 2013 WL 3788799 (D. Minn. July 18, 2013)). In *Yang Mee*, the court analyzed negligence *per se* allegations predicated on violations of Minn. Stat. §§ 580.02 and 580.05, sections that do not provide for liability and do not discuss what type of conduct would violate their provisions. The *Yang Mee* court unsurprisingly found no

"indication that §§ 580.02 and 580.05" could provide a basis for a negligence *per se* claim, and concluded that the plaintiff's claim was legally unfounded. *Yang Mee*, 2013 WL 3788799, at *2. *Yang Mee* has no bearing on this case because the PCSA, which expressly provides for civil liability, plainly meets the established criteria that courts apply to determine whether "negligence *per se* exists." *See Becerra Hernandez v. Flor*, No. 01-cv-183, 2002 WL 31689440, at *5 (D. Minn. Nov. 29, 2002) (Magnuson, J.)) (sustaining negligence *per se* claim).

C. Plaintiffs Have Adequately Alleged a Claim for Negligence.

Target's arguments concerning Plaintiffs' negligence claim attempt to rewrite the Complaint's allegations. This is not a case about Target's failure to protect Plaintiffs from an unforeseeable third-party criminal attack, and no "special relationship" is required to assert a claim of negligence under Minnesota law on the facts alleged. *Contra* Target Br. at 5-6; *see also* Target Br. at 13 n. 4 (citing case law holding that a merchant owes an issuing bank common law duty of care).

The Complaint plausibly alleges that Target acted negligently and harmed Plaintiffs in at least two ways: (1) by ignoring repeated warnings concerning the Breach as it was occurring and inexplicably turning off functions that could have prevented financial institutions from suffering millions of dollars in losses; and (2) by failing to protect card data in accordance with industry standards (and basic prudence), thus allowing the Breach to occur. There are no "new special relationship duties in tort" required, *see* Target Br. at 8, to hold negligent parties responsible for harm they inflicted upon foreseeable victims. *See Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys.*,

Inc., 729 F.3d 421, 426 (5th Cir. 2013) (reversing dismissal of card-issuing banks' negligence claim against defendant and finding that "***Heartland had reason to foresee the Issuer Banks would be the entities to suffer economic losses were Heartland negligent***"). This is especially so here, given that the Minnesota Legislature enacted the PCSA to supplement common law duties owed to financial institutions in cases of data breaches. *See* Minn. Stat. § 325E.64, Subd. 3 ("The remedies under this subdivision are ***cumulative*** and ***do not restrict*** any other right or remedy otherwise available to the financial institution"); *see also In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, MDL No. 2046, 2011 WL 1232352, at *23 (S.D. Tex. Mar. 31, 2011) (finding financial institutions are foreseeable victims of data breach because they are "identifiable, and the kinds of damages alleged—stemming primarily from card replacement and charging off fraudulent transactions—are straightforward").[4]

Notwithstanding the allegations in the Complaint, Target argues that Plaintiffs have not properly alleged two elements of negligence, duty and breach. *See* Target Br. 5-15. Notably, Target does not contest the sufficiency of Plaintiffs' allegations regarding the elements of injury or proximate cause (indeed, Target does not challenge Plaintiffs' causation and damages allegations with respect to any claim in the Complaint). As discussed below, Target's duty and breach are well-pled.

[4] The *Heartland* district court's dismissal of negligence claims under New Jersey's economic loss rule was reversed by the Fifth Circuit Court of Appeals. *See Lone Star*, 729 F.3d at 426.

1. Target Owed a Duty to Plaintiffs.

Negligence is the failure to exercise due or reasonable care. *See Rosen v. Edina Pub. Sch.-Indep. Sch. Dist. No. 273*, No. 13-cv-1704, 2014 WL 1661002, at *2 (Minn. Ct. App. Apr. 28, 2014). "The essential elements of a negligence claim are: (1) the existence of a duty of care; (2) a breach of that duty; (3) an injury was sustained; and (4) breach of the duty was the proximate cause of the injury." *Id.*

In the negligence context, duty is defined as "an obligation under the law to conform to a particular standard of conduct toward another." *Guin v. Brazos Higher Educ. Serv. Corp., Inc.*, No. 05-cv-668, 2006 WL 288483, at *3 (D. Minn. Feb. 7, 2006) (citing *Minneapolis Emps. Ret. Fund v. Allison-Williams Co.*, 519 N.W. 2d 176, 182 (Minn. 1994)). As this Court recently explained, Minnesota law looks to five factors when determining whether a defendant owed a plaintiff a duty of care: "(1) the foreseeability of harm to the plaintiff, (2) the connection between the defendant's conduct and the injury suffered, (3) the moral blame attached to the defendant's conduct, (4) the policy of preventing future harm, and (5) the burden to the defendant and community of imposing a duty to exercise care with resulting liability for breach." *Terry D. Fetterly v. Ruan Logistics Corp.*, No. 12-cv-2617, 2013 WL 6175181, at *3 (D. Minn. Nov. 25, 2013) (Magnuson, J.) (citing *Domagala v. Rolland*, 805 N.W.2d 14, 26 (Minn. 2011)).

Viewed in light of the five *Fetterly* factors, the allegations in the Complaint establish that Target owed Plaintiffs a duty of care to safeguard card data.

(a) The First *Fetterly* Factor Supports a Finding of Duty.

First, "the foreseeability of harm to the plaintiff" weighs overwhelmingly in favor of finding the existence of a duty here. Plaintiffs specifically allege both that (1) a card data breach like the one that occurred was probable if reasonable care were not exercised, and (2) it was clear that any such breach would cause harm to Plaintiffs. *See* ¶¶24-33, 43, 50-54, 67, 76-79, 103. Indeed, a data breach of Target's computer systems affecting card data was a known risk, and, as alleged, ***was actually warned-of as it occurred***. Specifically:

- Plaintiffs allege numerous prior breaches targeting sensitive card data and other payment information, which put the Company on notice that financial institutions could be harmed if Target failed to maintain reasonable security measures. ¶¶25-27.

- Plaintiffs allege that in 2013 Target received numerous warnings from the U.S. government, private research firms and Visa regarding the increasing frequency of sophisticated cyber-attacks on U.S retailers. ¶¶28-32. The warnings included specific recommendations for security measures that could minimize vulnerabilities to attacks, but "Target did not implement these measures." ¶32.

- Plaintiffs allege that ***in the months leading up to the breach "Target itself reported a 'significant uptick' in malware trying to enter its computer systems."*** ¶33.

- Plaintiffs allege that in September 2013, Target's employees raised specific concerns about security vulnerabilities in the Company's card systems, but that these concerns "went unheeded and Target officials ordered no further investigation." ¶43.

- Plaintiffs allege that Target received repeated alerts from its malware and antivirus security providers about the Breach as it occurred – *i.e.*, alerts that the breach was not just foreseeable, but ***was actually happening*** – but Target stood by and did nothing to prevent the disclosure of card data. ¶¶50-54, 59-60, 65, 67-69.

Plaintiffs also allege that Target was subject to: (1) regulations promulgated by credit and debit card companies and industry standards ("PCI DSS") that required Target to protect card data, ¶¶18-19; and (2) the PCSA, which regulated Target's maintenance of card data and "***was intended to address the very security deficiencies that led to the Target data breach***," ¶20, *see also* ¶¶21, 25, 25 n.1. These comprehensive regulations regarding Target's obligations to guard against data breaches like the one at issue further underscore the fact that such breaches are foreseeable occurrences.

It was also foreseeable that a data breach at Target would harm financial institutions that issued cards affected in the breach. First, the PCSA clearly identifies card-issuing financial institutions as entities that are foreseeably harmed in card data breaches. ¶¶20-22, 25 n.1, 115, 120. Indeed, the Act provides that a Minnesota business that violates the Act and suffers a data breach is liable to only one class of victims: financial institutions that issued cards affected by the breach. Minn. Stat. § 325E.64, Subd. 2 & 3. Aside from the Act, Plaintiffs also allege that Target had "specific notice" of the probability of harm "to financial institutions such as Plaintiffs" "if it failed to adequately protect its systems," including from, *inter alia*, experience with prior Point-Of-Sale terminal data breaches, and 2013 advisories from the Visa Corporation regarding malware that targeted cash register systems. ¶¶24-26, 30-32; *see also* ¶¶85-87, 103, 106.

Target urges the Court to "not even reach the issue of foreseeability" and to find instead that it had no duty to Plaintiffs because it did not have a "direct relationship" with them, but only with individual cardholders. Target Br. at 6-8. No "direct relationship" is required to establish a duty under negligence law. *See Fetterly*, 2013 WL 6175181, at *3.

Additionally, this argument is undermined by the PCSA, which requires violating businesses to compensate financial institutions for actions taken in response to data breaches "in order to protect the information of ***[their] cardholders*** or to continue to provide services to cardholders." Minn. Stat. § 325E.64, Subd. 3; *compare with* Target Br. at 12 ("The Banks repeatedly acknowledge that it was 'the personal and financial information ***of consumers***,' not the Banks, that allegedly was stolen.") (emphasis in original). The Act thus affirms the significance of Target's relationship with card-issuing banks and underscores Target's duty to Plaintiffs to safeguard card data.

Notably, courts adjudicating negligence claims in data breach cases have repeatedly held that card-issuing banks are foreseeable victims of card data security breaches. *See, e.g.*, *Lone Star*, 729 F.3d at 426 (reversing dismissal of negligence claim and holding that "Heartland had ***reason to foresee*** the Issuer Banks would be the entities to suffer ***economic losses*** were Heartland negligent"); *Digital Fed. Credit Union v. Hannaford Bros. Co.*, No. BCD-CV-10-4, 2012 WL 1521479, at *2, *4 (Me. B.C.C. Mar. 14, 2012) (plaintiff "is a ***foreseeable*** plaintiff insofar as [its] loss as an issuing bank is a foreseeable consequence of a data security breach by a merchant such as Hannaford"); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d 183, 194 (M.D. Pa. 2005) ("substantial harm" may come to card issuing banks from a merchant's negligence in connection with "its acceptance of credit and debit cards for retail transactions … and the ***harm is foreseeable***"); *see also Banknorth N.A. v. BJ's Wholesale Club, Inc*., 394 F. Supp. 2d 283, 286-87 (D. Me. 2005) (merchant owed a duty of care to card issuing bank "to safeguard cardholder information from thieves"). Such findings have rested, in part,

on the fact that the defendant communicated regularly with the issuing bank in the course of card transactions and was, therefore, well aware of the issuing bank's position. *E.g.*, *Lone Star*, 729 F.3d at 426 (finding that "the [plaintiff] Issuer Banks are the very entities to which [defendant] Heartland sends payment card information"); *Sovereign*, 395 F. Supp. 2d at 193 (finding that the defendant merchant "communicates directly with Sovereign before validating each transaction"). Like these cases, the Complaint alleges that Target communicated regularly with Plaintiffs in the course of card transactions, such that it was foreseeable that a card data breach would harm Plaintiffs. ¶¶17 (alleging that merchant such as Target "first seeks authorization from the issuing bank for the transaction[;] [i]n response, the issuing-bank informs the merchant whether it will approve or decline the transaction"), 103. The line of cases finding it foreseeable that card data security failures will injure card-issuing banks, and Plaintiffs' detailed allegations, demonstrate that "the foreseeability of harm to the plaintiff" is well-pleaded and plausible. *Fetterly*, 2013 WL 6175181, at *3.

(b) The Second *Fetterly* Factor Supports a Finding of Duty.

The second *Fetterly* factor, "the connection between the defendant's conduct and the injury suffered," *id.*, also weighs significantly in favor of a finding that Target owed Plaintiffs a duty to prevent the disclosure of card data. Plaintiffs allege a direct connection between Target's abject failures with respect to card data security, which allowed the Breach to happen, and Plaintiffs' injuries from costs associated with responding to the Breach. *See, e.g.*, ¶¶2, 15-16, 71-79, 86. Target, it bears noting, has not challenged Plaintiffs' allegations with respect to causation.

(c) The Final *Fetterly* Factors Support a Finding of Duty.

The final three *Fetterly* factors – "(3) the moral blame attached to the defendant's conduct, (4) the policy of preventing future harm, and (5) the burden to the defendant and community of imposing a duty to exercise care with resulting liability for breach" – also weigh in favor of finding that Target had a duty to Plaintiffs to protect card data. *Fetterly*, 2013 WL 6175181, at *3. Target's alleged conduct is morally blameworthy because, *inter alia*: (1) Target had exclusive control over Plaintiffs' vulnerable data but chose to ignore repeated security warnings and took none of the actions it easily could have taken to thwart the Breach before it inflicted any harm, *see* ¶¶30-32, 43, 50-55, 58-60, 67; and (2) Target chose to ***disable*** security functions that would have automatically deleted the malware in Target's system, thus actively enabling the Breach, *see* ¶¶50-55, 76-78. As alleged:

> 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***.

¶77. Moreover, in terms of moral blame, Plaintiffs had absolutely no ability to monitor or control Target's computer systems and no way of knowing about Target's security failures. Nonetheless, they are forced to absorb severe costs from Target's negligence. ¶¶1-2.

Whether moral blame attaches to conduct raises policy questions, and the fourth and fifth *Fetterly* factors also squarely implicate policy considerations. *Fetterly*, 2013 WL 6175181, at *3. The PCSA provides conclusive evidence of the Minnesota

Legislature's directive that merchants are required to secure card data and merchants failing to do so must compensate financial institutions in the event of a breach. ¶¶20-22, 25, 113-15. When determining questions of duty in other data breach cases, at least one court has looked for indicia of a legislative position as to whether a duty of care runs from the defendant to the plaintiff. *See Digital Fed. Credit Union*, 2012 WL 1521479, at *3 (although harm to card-issuing bank from merchant data breach was foreseeable, Maine public policy did not support finding a duty to issuing banks regarding data security because "to date, the [Maine] ***Legislature has not imposed a duty upon merchants for the benefit of issuing banks.***").

Notably, the five *Fetterly* factors are highly similar to the five factors analyzed by the U.S. District Court for the Middle District of Pennsylvania when determining the issue of duty and general negligence in another data breach action against a merchant brought by card-issuing banks. *Sovereign*, 395 F. Supp. 2d at 193 (analyzing duty by reference to (1) the parties' relationship, (2) the foreseeability of the harm incurred and the nature of the risk imposed, (3) the social utility of the conduct, (4) the consequences of imposing a duty on the actor, and (5) the public interest in the proposed solution). Applying this test, the *Sovereign* court held that the banks that issued BJ's customers' cards had alleged the existence of a duty in connection with their negligence claim. *Id.* While in subsequent rulings in *Sovereign* the otherwise valid negligence claim was dismissed, this was solely due to the application of Pennsylvania's economic loss doctrine. *See Sovereign Bank v. BJ's Wholesale Club*, 533 F.3d 162, 175 (3d Cir. 2008). Minnesota's economic loss doctrine, of course, has been highly circumscribed by statute,

see Ptacek v. Earthsoils, Inc., 844 N.W.2d 535, 538 (Minn. Ct. App. 2014) (citing Minn. Stat. § 604.101), applies only in cases of product defects, *id.*, and has no bearing on Plaintiffs' negligence claim (Target, tellingly, has not argued otherwise).

In sum, the *Fetterly* factors all support a finding of duty in this case. *See also Lone Star*, 729 F.3d at 426-27 (reversing dismissal of negligence claim by bank against card payment processor); *Sovereign*, 395 F. Supp. 2d at 193-95 (finding that merchant owed duty of care to card issuing bank); *Banknorth*, 394 F. Supp. 2d at 286-87 (rejecting merchant's argument that it "owed no duty of care" to card-issuing bank affected by breach of its card data systems and sustaining negligence claim).

2. Target Breached the Duty It Owed to Plaintiffs.

Target's argument that it should not be found to have breached any duties because Plaintiff's allegations are "conclusory," *see* Target Br. 14-15, simply ignores the relevant pleadings.

Plaintiffs allege that Target breached its duty to Plaintiffs when it chose to take none of the myriad actions it could have taken, even upon repeated warnings, to prevent the Breach. *See* ¶¶30-32, 43, 50, 53-55, 58-60, 67, 76-78. Target does not contest these allegations; rather, "Target has admitted [that] the Company had multiple opportunities to identify and prevent the attack on its data systems, but key personnel at Target remained unaware or unconcerned about what had occurred…." ¶67. The Senate Report made similar findings. ¶78.

Plaintiffs also allege that Target failed to adhere to applicable industry standards, or even basic prudence, in its data security activities. For example: (1) as reported by

Bloomberg, Target ***intentionally*** turned off a malware security function that would have automatically deleted any malware detected prior to the Breach (¶77); (2) "Target did not implement" numerous security measures recommended by Visa to enhance the security on the specific operating system Target employed in connection with accepting payment cards (¶¶30-32); (3) Target could have, but failed to, implement measures called for under PCI-DSS 2.0, which was operative in November 2013 (¶52); and (4) Target retained sensitive card data, in direct violation of both industry norms and the PCSA, at the time of the Breach (*e.g.*, ¶¶75, 82-84).

These allegations of breach are not "conclusory," but describe in detail conduct that is unmistakably negligent. *See Banknorth*, 394 F. Supp. 2d at 284 (sustaining card-issuing bank's negligence claim against merchant based on theory that "due to [merchant's] failure to protect and secure the Visa card magnetic stripe information that it retained, unauthorized third parties" were able to steal such information); *Lone Star*, 729 F.3d at 423, 426-27 (reversing dismissal of negligence claim by card-issuing bank against defendant that failed to secure card data). At minimum, Target's contention that no standard of reasonable conduct was breached raises fact questions that cannot be resolved on a motion to dismiss. *See Banknorth*, 394 F. Supp. 2d at 286.

3. Plaintiffs Have Also Adequately Alleged a Special Relationship Between Target and Plaintiffs.

As set forth above, Plaintiffs have adequately established at this stage of proceedings that Target owed Plaintiffs a duty of care regarding card data security under Minnesota's general negligence law. Plaintiffs therefore need not establish a "special

relationship" to prevail on their negligence claim. Nevertheless, the Complaint also adequately alleges the existence of a "special relationship" between Target and financial institutions.

(a) Target Was the *Only* Party Able to Protect Plaintiffs.

While traditionally a "special relationship" giving rise to a duty is recognized on the part of common carriers, innkeepers, possessors of land who hold their land open to the public, and persons who have custody of another where the other does not have the normal opportunity for self-protection, Minnesota courts have recognized a special relationship in circumstances where the defendant is a merchant. *See, e.g.*, *Erickson v. Curtis Inv. Co.*, 447 N.W.2d 165, 169 (Minn. 1989) (imposing on parking facility owner a duty to protect customers from criminal harm). Courts may find a special relationship exists 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). To conclude "that a special relationship exists, it must be assumed that the harm to be prevented by the defendant is one that the defendant is in a position to protect against and should be expected to protect against." *Id.* "Ultimately, the question is one of policy." *Erickson*, 447 N.W.2d at 169.

The Complaint alleges that Plaintiffs, financial institutions that issued payment cards used at Target, were vulnerable to and dependent upon Target with respect to the safekeeping of card data. ¶¶1, 2, 18-19, 22, 61-63, 71-78. Target contends its duties to safeguard card data ended when third-parties – hackers – struck, but this argument

obscures Plaintiffs' allegations that Target's gross security deficiencies enabled the Breach, and Target's inaction and omissions worsened the Breach's effect on Plaintiffs. Hackers' activities do not excuse Target from properly securing card data – as alleged, hackers' activities are a given, assumed by statute, and a fundamental reason why Target is obligated to maintain data security in the first place. ¶¶18-20, 24-33. Once customers used credit and debit cards to make purchases at Target, this confidential financial information was in Target's custody and control. Plaintiffs were then dependent on Target to safeguard and delete the information as required by prudence and the PCSA. Plaintiffs had no ability to protect information in Target's possession nor could Plaintiffs know that Target's systems were breached. *See e.g.*, ¶¶1-2, 14-15, 24-60, 65-69, 77.

Target, and only Target, was in a position to stop the Breach and to safeguard sensitive card data. For example:

- Target had full control of its computer network and determined how to secure it. ¶¶28, 34.
- Target could have configured and secured its system and prevented the Breach. *See, e.g.*, ¶77 (Target turned off security function which automatically deletes malware); ¶¶47-48 (Target failed to segment its computer systems and require two-factor authentication for vendors); ¶52 (Target could have prevented breach by eliminating unneeded default accounts and requiring vendors to monitor their systems); ¶59 (Target could have prevented transmission of information by hackers by only allowing its network to upload to approved servers).
- Target was also in a position to stop the Breach before the hackers loaded malware onto Target's system, when Visa warned Target about RAM-scraper malware and members of Target's security staff raised alarms about the system's vulnerability. ¶¶30-32, 43, 77.
- Target had further opportunities to stop the Breach once underway. ¶¶49-51, 53-60.

Plaintiffs thus allege that Target had complete control over the card data subsequent to customer transactions, and had the exclusive ability to prevent the hackers from perpetrating the Breach. *Cf. Becker v. Mayo Found.*, 737 N.W.2d 200, 213 (Minn. 2007) (no special relationship existed between hospital and child abuse victim where defendant-hospital did not exercise control over victim's daily welfare and noting that "cases recognizing a special relationship … all involve some control by the defendant over the harm-causing agent"). These facts are sufficient to demonstrate a special relationship. *See Erickson*, 447 N.W.2d at 169 (holding that where circumstances "present a … unique opportunity for criminals and their criminal activities" and that "[s]ome duty is owed").

The special relationship between a possessor of land and an invitee is also instructive. *Tiedeman By & Through Tiedeman v. Morgan*, 435 N.W.2d 86, 88 (Minn. Ct. App. 1989) ("an invitee upon the premises of another is 'entitled to a higher degree of care than those who are present by mere sufferance.'"). Although liability to an invitee who suffers a third-party criminal act on the defendant's premises is not automatic, if a "physical condition of the store premises" presents an "opportunity to criminals" not available outside the premises, a duty to protect may be found. *Errico v. Southland Corp.*, 509 N.W.2d 585, 588 (Minn. Ct. App. 1993). Here, Target's computer network, as operated – including Target's decisions to turn off the automatic deletion of malware and ignore the warnings of its security and antivirus providers – created a clear and unique opportunity for hackers to install malware and steal card data. ¶¶43, 49-51, 53-

60, 77-78. Accordingly, Plaintiffs have plausibly alleged that Target had a "special relationship" to Plaintiffs.

(b) The Harm Was Foreseeable.

As set forth above, *see* Section IV.C.1, *supra*, the harm Plaintiffs suffered from the data breach was foreseeable.

(c) Economic Losses Are Compensable Where a Special Relationship Exists.

Target suggests that a "special relationship" cannot exist in actions for economic losses or relationships deriving from commercial transactions. *See* Target Br. at 9-10. This argument is contrary to Minnesota law.

First, as set forth above, the standard applied by Minnesota courts to determine the existence of a "special relationship" does not consider the nature of the losses or the transaction underlying the dispute. Instead, Minnesota courts focus solely on the relationship between the parties. *See United Prods. Corp. of Am. v. Atlas Auto Parts, Inc.*, 529 N.W.2d 401, 404 (Minn. Ct. App. 1995) ("To have a special relationship and a duty to protect… appellant needed to have entrusted its safety to respondent, respondent needed to have accepted that responsibility, and respondent had to have the ability to protect against the harm the vandals created."); *see also Donaldson*, 539 N.W.2d at 792.

Second, Target cannot cite a single Minnesota decision that prohibits finding a "special relationship" in a case involving only economic loss or commercial transactions as a matter of law. *See* Target Br. at 10. However, the Minnesota Supreme Court has found a special relationship in a case where the basis for the plaintiff and defendant's

relationship was commercial. *See Erickson*, 447 N.W.2d at 169 (finding special relationship between merchant and customer in imposing duty to use reasonable care in deterring criminal activity at parking ramp). Thus, contrary to Target's assertion, commercial transactions ***may*** give rise to "special relationships" under Minnesota law.

The cases cited by Target for the contrary proposition are factually distinguishable. *See Superior Constr. Servs., Inc. v. Moore*, No. A06-1491, 2007 WL 1816096, at *3-4 (Minn. Ct. App. June 26, 2007) (finding no special relationship where plaintiff did not entrust its safety to defendant and defendant did not accept responsibility); *United Prods. Corp. of Am., Inc. v. Atlas Auto Parts, Inc.*, 529 N.W.2d 401 (Minn. Ct. App. 1995) (same); *Mack v. Britto Cent., Inc.*, No. 13-197, 2013 U.S. Dist. LEXIS 110142, at *25 (D. Minn. Aug. 6, 2013) (declining to impose a duty where plaintiff did not allege any facts necessary to establish "special relationship"). Here, Plaintiffs have alleged facts establishing that Target was entrusted with confidential information and that Target accepted the responsibility for safekeeping the information.

Furthermore, contrary to its assertion (Target Br. at 6-7 n.3), Target has caused physical damage to Plaintiffs' property. The cards compromised in the Breach were owned by Plaintiffs, and Plaintiffs' customers had to destroy the cards to mitigate the effects of the Breach. Plaintiffs then had to create new account information and issue replacement cards. ¶85 (alleging financial institutions are "primarily responsible for paying for card replacement"); ¶86 (financial institutions were forced to dedicate significant capital and human resources to reissuing cards and changing or closing accounts). Plaintiffs' losses thus include the physical replacement of cards irreparably

damaged by Target's actions and inactions. *See* Minn. Stat. § 325.64, Subd. 3 (providing damages for, *inter alia*, cost of card replacement).

(d) Target Voluntarily Assumed a Duty to Protect Plaintiffs From the Breach.

The Minnesota Supreme Court recently recognized that "[o]ne who voluntarily assumes a duty must exercise reasonable care, even if he is not otherwise obligated to provide the care, or he will be responsible for damages resulting from his failure to do so." *See Glorvigen v. Cirrus Design Corp.*, 816 N.W.2d 572, 584 (Minn. 2012). The voluntary duty doctrine applies not only to personal injury claims, but also to property damage. *See Abresch v. Nw. Bell Tel. Co.*, 75 N.W.2d 206, 211 (Minn. 1956).

Target assumed the duty to detect and protect against the very type of malware that caused Plaintiffs' losses. In February 2013, Target hired FireEye, a renowned security software company, to update Target's computer security systems. ¶34. FireEye provided Target with state-of-the-art malware detection tools, including security specialists who continuously monitored Target's systems. Target, however, actively neutralized its malware security, as it ignored repeated alerts regarding malware, and turned off a function that automatically deleted it. ¶¶30-32, 49-51, 53-60, 77-78. Thus, Plaintiffs have plausibly alleged that Target is liable under the voluntary duty doctrine.

Target cites *Funchess v. Cecil Newman Corp.*, 632 N.W.2d 666 (Minn. 2001), for the proposition that it owed no duty to anyone to maintain its security system. *See* Target Br. at 15 n.6. Target misinterprets *Funchess*, which did not provide blanket immunity to businesses in cases involving third party criminal conduct. *See Funchess*, 632 N.W.2d at

675 ("there may be other circumstances in which the duty to maintain security measures would give rise to liability"). *Funchess* concerns, *inter alia*, whether a landlord assumed a duty to protect a tenant by maintaining a lock on a common entryway. *Id.* at 675. The court concluded the landlord had no duty to maintain the lock because the lock protected the building in general – the plaintiff-tenant had a lock on his apartment to protect himself – and because the landlord had provided other security measures for the tenant's benefit – a guard who chased the assailants away. *Id*. Here, the core function of Target's security system was to protect confidential card data. *See, e.g.*, ¶¶18-20, 22, 28, 34, 36, 44, 50, 53-54. Critically, unlike *Funchess*, there were no measures that Plaintiffs could take to protect card data subsequent to a transaction with Target, and Target failed to act when notified of the attack. Accordingly, *Funchess* is distinguishable.

4. The Minnesota Plastic Card Security Act Does Not Limit Plaintiffs' Common Law Remedies.

Target inexplicably argues that the PCSA should prevent this Court from recognizing any tort duty owed to Plaintiffs. Target Br. at 8. This argument runs counter to the Act's plain language, which explicitly provides that the Act does not limit other rights or remedies available to financial institutions, necessarily including common law remedies. *See* Minn. Stat. § 325E.64, Subd. 3 ("remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution").

Moreover, Target cites no law for the proposition that legislation displaces common law rights addressing similar subject matter. Minnesota courts have held the

exact opposite. *See Larson v. Wasemiller*, 738 N.W.2d 300, 311 (Minn. 2007) ("Under the rules of statutory construction generally recognized by this court, a statute will not be construed to abrogate a common law right unless it does so expressly."); *Haage v. Steies*, 555 N.W.2d 7, 8 (Minn. Ct. App. 1996) ("Unless a statute manifests a legislative intent to modify, statutes are presumed not to alter the common law."). Financial institutions' common law rights against merchants with respect to card data security are confirmed by other data breach cases. *See* Section IV.C.1 *supra*. The proposition that the PCSA limits common law tort duties that Target owes Plaintiffs is baseless.

5. The Visa and MasterCard Operating Regulations Do Not Obviate Plaintiffs' Claims.

Target attaches to its Motion the Visa and MasterCard Card Operating Regulations ("Regulations") and suggests that they preclude Plaintiffs from seeking tort remedies from Target for harm suffered as a result of the breach. Target Br. at 11-12. Target's argument misses the mark. The Regulations do not conclusively establish that Plaintiffs had an exclusive contractual remedy for the harm suffered as a result of the Breach. Initially, the Regulations themselves nowhere limit a card-issuing bank's common law remedies when harmed by a security breach. *See generally* ECF No. 186 ("Meal Decl."), Exs. A and B.[5] Courts in other data breach cases have rejected arguments at the motion

[5] In any case, the Regulations do not immunize Target given that they provide a compensation mechanism for losses that may be caused by an ***Acquirer bank's*** actions. Indeed, the Visa Regulations discuss how an "issuer… may recover a portion of its Incremental Counterfeit Fraud losses and operating expenses… ***from an Acquirer***(s) to whom liability for such loss has been assigned under the GCAR program." Visa Operating Regulations at *676 (Meal Decl. Ex. A). Plaintiffs do not allege that Target is an "Acquirer" under the Visa Regulations. Likewise, in the MasterCard Regulations

to dismiss stage suggesting that the Regulations preclude tort claims by financial institutions. *See, e.g.*, *Sovereign*, 395 F. Supp. 2d at 195 (argument that contract-based Visa system precludes issuer bank's negligence claim "is not persuasive"); *Lone Star*, 729 F.3d at 426 ("any contractual remedies the Issuer Banks have to recoup losses … are not evident").

Moreover, the significance of the Regulations, which are not contracts between Plaintiffs and Target, is a factual issue, inappropriate for disposition at this stage. *See e.g. Banknorth*, 394 F. Supp. 2d at 287 (denying motion to dismiss card-issuing bank's negligence claim and finding that "credit card industry involves a complex web of relationships involving numerous players" that implicate "issues of fact … that the Court may not appropriately resolve via a motion to dismiss"). As such, Target's Regulations-based argument should be rejected.

The absence of contractual duties or privity between Plaintiffs and Target in fact underscores, rather than undercuts, Target's duties in tort. *See, e.g.*, *Oriental Trading Co. v. Firetti*, 236 F.3d 938, 945 (8th Cir. 2001) (where plaintiff did not seek remedies based on contract to which defendants were not parties, but instead sought return of money advanced in reliance on defendants' statements, plaintiff could proceed on tort claims and other contracts were "irrelevant"); *TCF Nat. Bank v. Mkt. Intelligence, Inc.*, No. 11-2717

---

partial incremental losses may be available "based on the amount collected from the responsible Customer," with "Customer" defined as "***a financial institution*** or other entity that has been graded a License in accordance with the Standards." MasterCard Security Rules and Procedures, Merchant Edition (August 30, 2013), at § 10.2.5.3 (Meal Decl., Ex. B). The Complaint does not allege that Target is a "Customer" under the MasterCard Regulations. Defendant's reliance on these agreements is misplaced and raises factual issues that cannot be resolved at present.

JRT/AJB, 2012 WL 3031220, at *4 (D. Minn. July 25, 2012) (even in context of parties with direct privity of contract, tort duties that exist independent of contract are actionable, particularly where plaintiff "could have brought them even if no contract existed"); *Wolfram v. S.K. Fin. Servs., Inc.*, No. C7-95-1778, 1996 WL 70308, at *4 (Minn. Ct. App. Feb. 20, 1996) (observing that courts typically invoke tort duty when contract contemplates unidentified parties that cannot surmount hurdles of contractual privity or promissory estoppel).

In sum, Plaintiffs have plausibly alleged that Target had a duty to Plaintiffs – under Minnesota's general negligence jurisprudence, and, alternatively, under its "special relationship" standards – and breached it. Plaintiffs' negligence claim is well-pleaded.

D. Plaintiffs Have Adequately Alleged a Negligent Misrepresentation by Omission Claim.

Target attempts to miscast Plaintiffs' claim for negligent misrepresentation by omission as a claim asserting an affirmative negligent misrepresentation. *See* Target Br. at 16. Target again ignores the Complaint's allegations. *See, e.g.*, ¶¶18-19, 60, 65, 68, 82, 128-34.

To establish a claim for negligent misrepresentation by omission, a plaintiff must show that "the defendant has failed to communicate 'certain information that the ordinary person in his or her position would have discovered or communicated.'" *Heffron v. Burlington N. & Santa Fe Ry. Co.*, No. 08-cv-5194, 2008 WL 5273711, at *2 (D. Minn. Dec. 17, 2008) (quoting *Safeco Ins. Co. of Am. v. Dain Bosworth, Inc.*, 531 N.W.2d 867, 870 (Minn. Ct. App. 1995)). Normally, "[t]his duty of care arises when the defendant

'suppl[ies] information for the guidance of others in the course of a transaction in which [he] has a pecuniary interest, or in the course of [his] business. . . .'" *Id.* However, Minnesota law recognizes "special circumstances may trigger a duty to disclose material facts." *Graphic Commc'ns Local 1B Health & Welfare Fund "A" v. CVS Caremark Corp.*, 850 N.W.2d 682, 695 (Minn. 2014); *see also* Target Br. at 17 (noting that "special relationship" may trigger disclosure duty). "Special circumstances" include cases where "one who has special knowledge of material facts ***to which the other party does not have access***" and when the speaker "must say enough to prevent the words communicated from misleading the other party." *Graphic Commc'ns*, 850 N.W.2d at 695. The Supreme Court of Minnesota has cautioned that examples of "special circumstances" in Minnesota case law are "***not intended to be exclusive***." *Id.*

1. Plaintiffs Have Adequately Alleged Duty and Misrepresentations by Omission.

Plaintiffs have alleged particularized facts supporting that Target owed them a duty of care to disclose material facts about Target's inadequate data security systems well before December 19, 2013.

Specifically, Plaintiffs allege that Target had knowledge of, but failed to disclose, deficiencies in its data security practices including its decision to turn off malware detection software that would have prevented Plaintiffs' losses. *See* ¶¶30-32, 43, 50, 53-54, 60, 65, 77, 127-31. Plaintiffs were dependent on Target for the safekeeping of confidential card data within Target's custody and control. ¶¶1-2, 18-19, 22, 61-63, 71-75, 77-78. Further, Target was the ***only party*** capable of knowing that its systems were

deficient and open to being compromised. ¶¶2, 14-15, 24-60, 65-69, 77. Target was thus in possession of "special knowledge" regarding its data security, which was not and could not have been known to Plaintiffs. This special knowledge imposed an affirmative duty of disclosure on Target. *See Graphic Commc'ns*, 850 N.W.2d at 695.

Separately, Plaintiffs also allege that through Target's Privacy Policy, which is published on its website, Target voluntarily provided assurances about its data security systems. *See* ¶¶128-29; *see also* Declaration of J. Gordon Rudd, Jr., Exhibit A at *5, ("When we collect or transmit . . . credit or debit card number, ***we use industry standard methods to protect that information***"). By making these voluntary assurances, Target assumed a duty of full disclosure. *See Graphic Commc'ns*, 850 N.W.2d at 695 (choosing to speak triggers duty of full disclosure); *M. H. v. Caritas Family Servs.*, 488 N.W.2d 282, 288 (Minn. 1992) (same); *cf. In re TJX Cos. Retail Sec. Breach Litig.*, 524 F. Supp. 2d 83, 91-92 (D. Mass. 2007) (sustaining claim based on "implied representations that TJX … made to the issuing banks that [TJX] took the security measures required by industry practice to safeguard" card data); *Freedman v. St. Jude Med., Inc.*, No. 12-cv-3070, 2014 WL 910326, at *18 (D. Minn. Mar. 10, 2014) (half-truths are actionable misrepresentations).

Target's attempt to recast this case as one involving an "arm's length commercial" relationship, *see* Target Br. at 17-18, is baseless. Target and Plaintiffs were *not* involved in any arm's-length transactions. Plaintiffs were fully dependent on Target to secure sensitive card data. Accordingly, Target's cited authorities failing to impose disclosure duties in commercial transactions, *see* Target Br. at 17-18, are inapposite. *See*

Huntington Bancshares, Inc. v. Ally Fin., Inc., No. 27-11-cv-20276, 2012 WL 7749245 (Minn. Dist. Ct. Dec. 11, 2012) (noting parties' "arm's length transaction"); *Regions Treatment Ctr., LLC v. New Stream Real Estate, LLC*, No. 13-cv-1752, 2014 WL 107792 (D. Minn. Jan. 10, 2014) (same).[6]

2. Plaintiffs Need Not Allege Reliance.

Contrary to Target's arguments, Target Br. at 25-26, Plaintiffs have only pled that Target failed to disclose material weaknesses in its data security systems that it had an obligation to disclose. ¶¶128-34. Pleadings of reliance in the context of negligent misrepresentation by omission are not required. *Smith v. Questar Capital Corp.*, No. 12-cv-2669, 2014 WL 2560607, at *15 (D. Minn. June 6, 2014) (sustaining negligent misrepresentation by omission claim). Neither of the cases cited by Target, *Raden v. BAC Home Loans Servicing, LP*, No. 12-cv-1240, 2013 WL 656624, at *4-5 (D. Minn. Feb. 22, 2013), nor *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 594 (S.D. Tex. 2011), addressed omissions, and so these cases are distinguishable. Plaintiffs' allegations are based on Target's omission of material information it was under a duty to disclose – not on material misstatements – and accordingly, this claim should be sustained. *See* ¶¶128-34.

[6] To the extent the pleading requirements of Fed. R. Civ. P. 9(b) apply to negligent omission claims, Plaintiffs have satisfied Rule 9(b) by "identify[ing] the who, what, where, when, and how of the alleged" negligent misrepresentation by omission. *Petsche v. EMC Mortg. Corp.*, 830 F. Supp. 2d 663, 673 (D. Minn. 2011). Specifically, the Complaint alleges that Target negligently omitted that it did not follow industry protocols to secure payment data and that it intentionally disabled malware prevention software prior to accepting Plaintiffs' cards in its stores. These allegations "enable the defendant to respond specifically and quickly" to Plaintiffs' claim. *See United States ex rel. Costner v. United States*, 317 F.3d 883, 888 (8th Cir. 2003).

V. CONCLUSION

For the foregoing reasons, Target's motion should be denied in its entirety.

Dated: October 1, 2014

ZIMMERMAN REED, PLLP

By: /s/ Charles S. Zimmerman
Charles S. Zimmerman (MN 120054)
J. Gordon Rudd, Jr. (MN 222082)
Brian C. Gudmundson (MN 336695)
1100 IDS Center
80 South 8th St.
Minneapolis, MN 55402
Telephone: (612) 341-0400
charles.zimmerman@zimmreed.com
gordon.rudd@zimmreed.com
brian.gudmundson@zimmreed.com

Lead Counsel for Financial Institution Plaintiffs

CHESTNUT CAMBRONNE PA
Karl L. Cambronne (MN 14321)
Jeffrey D. Bores (MN 227699)
Bryan L. Bleichner (MN 0326689)
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
kcambronne@chestnutcambronne.com
jbores@chestnutcambronne.com
bbleichner@chestnutcambronne.com

Coordinated Lead Counsel for Plaintiffs

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen Hanson Riebel (MN 219770)
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com

Bank Liaison Counsel

REINHARDT WENDORF & BLANCHFIELD
Garrett Blanchfield (MN 209855)
E-1250 First National Bank Building
332 Minnesota Street
St. Paul, MN 55101
Telephone: (651) 287-2100
g.blanchfield@rwblawfirm.com

Coordinating Liaison Counsel

LEVIN, FISHBEIN, SEDRAN & BERMAN
Howard J. Sedran
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
hsedran@lfsblaw.com

KESSLER TOPAZ MELTZER & CHECK LLP
Naumon A. Amjed
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
namjed@ktmc.com

SCOTT + SCOTT LLP
Joseph P. Guglielmo
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Telephone: (212) 223-6444
jguglielmo@scott-scott.com

HAUSFELD LLP
James J. Pizzirusso
1700 K Street NW, Suite 650
Washington D.C. 20006
Telephone: (202) 540-7200
jpizzirusso@hausfeldllp.com

Plaintiffs Leadership Committee

BARRETT LAW GROUP, P.A.
Don Barrett
404 Court Square North
PO Box 927
Lexington, MS 39092
Telephone: (662) 834-9168
dbarrett@barrettlawgroup.com

CARLSON LYNCH LTD
Gary F. Lynch
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Telephone: (412) 322-9243
glynch@carlsonlynch.com
sfellows@carlsonlynch.com

BEASLEY, ALLEN, CROW, METHVIN, PORTIS MILES, P.C.
W. Daniel Miles, III.
272 Commerce Street
PO Box 4160
Montgomery, AL 36103-4160
Telephone: (334) 269-2343
dee.miles@beasleyallen.com