UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

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

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,

vs.

Target Corporation,

Defendant.

DEFENDANT'S MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Target Corporation ("Target") submits this memorandum of law in support of its Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint ("Complaint").

I. SUMMARY OF PERTINENT FACTUAL ALLEGATIONS

A. The Criminal Intrusion on Target's Computer Network.

On December 19, 2013, Target announced that it had been the victim of a criminal attack on its computer network by third-party intruders (the "Intrusion"), which had been confirmed only four days earlier. Compl. ¶ 68 n.2. The Intrusion was carried out by sophisticated criminal hackers (Compl. ¶ 103), who gained access to Target's network through credentials they stole from a third-party vendor whom Target retained for HVAC maintenance. Compl. ¶¶ 41, 46. Once inside the Target network, the hackers deployed custom point-of-sale malware to Target's registers, which collected credit and debit card (jointly, "payment card") information "in real time" when customers swiped their cards at Target registers between December 2, 2013 and December 15, 2013. Compl. ¶¶ 49, 56.

Target's security measures were certified by an independent auditor as compliant with "all payment industry requirements" and included "state of the art" tools that Target invested substantial resources to acquire. Compl. ¶¶ 28, 34, 44. However, plaintiffs – a group of five payment-card-issuing banks, credit unions, and savings associations (the "Banks") (Compl. ¶¶ 7–12) – nonetheless assert that Target is to blame for not preventing the Intrusion. Compl. ¶¶ 2, 86. They claim resulting financial losses that include costs associated with reissuing payment cards to customers and reimbursing fraudulent charges. *Id*.

B. The Parties and Their Roles in the Payment Card Networks.

The Banks are headquartered in Oregon, Massachusetts, Minnesota, Louisiana, and Ohio. Compl. ¶¶ 7–12. Target is a Minnesota corporation with retail locations throughout the United States. Compl. ¶¶ 13–14.

Payment card issuers like the Banks participate in an "extensive network of financial institutions" that together process retail payment card transactions. Compl. ¶ 18. This process begins with a financial institution, like the Banks, issuing a payment card to a consumer. The consumer then may choose to use that payment card to make purchases at retail merchants, such as Target. Compl. ¶ 17. When this occurs, the merchant obtains authorization and payment for the transactions not from the bank that issued the card (the "issuing bank"), but rather from a payment processor and/or a merchant bank (an "acquiring bank") that has contracted with the merchant to handle the transaction. *Id.* The acquiring bank in turn obtains authorization and payment under its separate contract with a payment card company such as Visa and MasterCard (the "Card Brands"), and the Card Brand in turn obtains authorization and funding under its separate contract with the issuing bank.[1] Thus, issuing banks and merchants have no direct dealings with one another in the payment card transaction process.

[1] *See* Visa International Operating Regulations (Oct. 15, 2013), at *49, *51, *941, *1019 (Decl. of Douglas H. Meal ("Meal Decl."), Ex. A) (providing that acquirers and issuers are both "Members" who contract with Visa and are subject to Visa's Operating Regulations). Because the Card Operating Regulations are "necessarily embraced by the pleadings," *see, e.g.*, Compl. ¶¶ 17–18, the Court may consider them on a motion to dismiss. *Twin City Sprinkler Fitters v. Total Fire Prot., Inc.*, No. Civ. 02-930 PAMRLE, 2002 WL 31898170, at *1 n.1 (D. Minn. Dec. 26, 2002). *See also Banknorth v. BJ's*

The Card Brands have issued comprehensive regulations governing these processes ("Card Operating Regulations"). Compl. ¶ 18. Although merchants do not contract directly with the Card Brands, the Banks allege that the Card Operating Regulations are incorporated into merchants' contracts with acquiring banks. *Id.* The Banks also allege that merchants are contractually bound to comply with the Payment Card Industry Data Security Standard ("PCI-DSS"), which sets forth information security requirements by the Payment Card Industry Security Standards Council, through an unspecified agreement. *Id.* ¶¶ 19, 129.

II. SUMMARY OF THE ARGUMENT

In their Complaint, the Banks assert counts for negligence (Compl. ¶¶ 100–11) and negligent misrepresentation by omission (Compl. ¶¶ 127–34), as well as for violation of the Minnesota Plastic Card Security Act (the "PCSA") (Compl. ¶¶ 112–20) and negligence *per se* based on the PCSA (Compl. ¶¶ 121–26). Each is fundamentally flawed.

The Banks' negligence and negligent misrepresentation claims hinge, among other things, on there being a never-before recognized "special relationship" between merchants, like Target, and payment card issuers, like the Banks, that justifies creation and imposition of a novel *common-law* duty of care. The Banks, however, are sophisticated parties that do not even have a *direct* relationship with Target, much less a *special* relationship that might suffice to create such a duty in either the negligence or negligent misrepresentation context. Especially since (i) the Minnesota Legislature

---

Wholesale Club, Inc., 442 F. Supp. 2d 206, 213 (M.D. Pa. 2006) (noting that issuing banks operate through a contract with a Card Brand).

already has addressed the issue of when a merchant might be liable to an issuer following a data breach; (ii) the contractual regime upon which the Banks base many of their claims *already* provides a system under which issuers may be compensated following a data breach; and (iii) courts in other jurisdictions *already* have refused to impose common-law tort duties based on similar allegations, the facts alleged here do not justify the imposition of new and unprecedented common-law tort duties under Minnesota law. Even if that were not the case, the Banks' failure to plead other elements of their claims, such as breach, an actionable misrepresentation by omission, or reliance, would nonetheless require dismissal.

In an attempt to plead around these fatal defects, the Banks resort to the PCSA and an accompanying negligence *per se* claim. But neither can save the Banks' Complaint, since the Banks' own allegations confirm that the Intrusion involved theft of payment card data "in real time," and thus did not involve a PCSA violation.

III. LEGAL STANDARD

To withstand a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a plaintiff must proffer more than mere "labels and conclusions," but rather must allege sufficient factual matter to "raise a right to relief above the speculative level." *Peterson v. Argent Mortg. Co.*, No. 06-3796, 2007 WL 1725355, at *1 (D. Minn. June 14, 2007) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

IV. ARGUMENT

A. The Banks' Negligence Claim Must Be Dismissed.

Count I of the Complaint asserts a claim for negligence. To state a claim for negligence under Minnesota law,[2] a plaintiff must allege (1) the existence of a duty, (2) breach of that duty, (3) proximate cause, and (4) injury. *See, e.g.*, *Johnson v. State*, 553 N.W.2d 40, 49 (Minn. 1996).

The Banks have failed to plead that Target owed the Banks any duty of care or that Target breached any such duty, the absence of either of which requires dismissal.

1. *The Banks Fail to Plead that Target Owed Them a Duty of Care.*

The existence of a duty of care is a threshold requirement for negligence – absent a legal duty, the Banks' claim fails. *See, e.g.*, *id.* at 50. In the Complaint, the Banks variously allege that Target owed them a duty in "obtaining, retaining, securing, and deleting" payment card information that Target collects from its consumers, providing security for that information consistent with industry standards, and thwarting intrusions "routinely attempted" by "sophisticated hackers." *See* Compl. ¶¶ 101–103, 106. No matter how the Banks cast their assertions of duty, however, they all boil down to the contention that a merchant has a *common-law* duty to take certain steps to protect issuing banks from financial losses caused by third-party criminal attacks aimed at stealing payment card data. Minnesota law recognizes no such duty.

[2] Because the Complaint nowhere purports to differentiate between the laws applicable to the five Banks' claims, Target assumes for purposes of this motion to dismiss, without conceding, that Minnesota law applies to all of the Banks' common-law claims.

"As a general rule, a person has no duty under Minnesota law to protect another from the harmful conduct, including criminal conduct, of a third person." *RKL Landholding, LLC v. James*, No. A12-1739, 2013 WL 2149979, at *2 (Minn. Ct. App. May 20, 2013) (citing *Donaldson v. Young Women's Christian Ass'n of Duluth*, 539 N.W.2d 789, 792 (Minn. 1995)). This is so even when "an actor realizes or should realize that action on his part is necessary for another's aid or protection." *Johnson*, 553 N.W.2d at 49. Instead, a duty to protect against third-party criminal harm arises only where (i) there is a special relationship between the defendant and the plaintiff (or the defendant and the third party); *and* (ii) the third-party harm is foreseeable. *Clark ex rel. H.B. v. Whittemore*, 552 N.W.2d 705, 707 (Minn. 1996). Here, the Court need not even reach the issue of foreseeability, because the Banks plead no facts in support of their conclusory assertion that "Target maintained a special relationship" with them (Compl. ¶ 104). *See Johnson*, 553 N.W.2d at 50 (holding that the court "need not reach the issue of foreseeability" where the plaintiffs failed to plead the requisite special relationship).[3]

[3] Minnesota also recognizes that an actor owes a limited duty to protect another from its *own* misfeasance – i.e., "active misconduct working positive injury to others," *see* W. Page Keeton et al., *Prosser and Keeton on the Law of Torts* § 56 (5th ed.1984); *see also Catlin Underwriting Agencies*, No. A13-2078, 2014 WL 3800595, at *5 (Minn. Ct. App. Aug. 4, 2014) – but the Complaint's assertions about "Target's own conduct" (Compl. ¶ 106) amount to nothing more than claims of nonfeasance: that Target failed to take steps that may have stopped the third-party criminal attackers from doing harm. *See BancFirst v. Dixie Rests., Inc.*, No. CIV-11-174-L, 2012 WL 12879, at *4 (W.D. Okla. Jan. 4, 2012) (allegations of a merchant's failure to prevent a data breach do not suffice as "affirmative acts"). Minnesota also recognizes that an actor may voluntarily undertake (or assume) a duty which otherwise does not lie, but only where plaintiffs allege property damage or personal injury. *See, e.g., United HealthCare Ins. Co. v. Advance PCS*, No. Civ.01-2310 (RHK/AJB), 2003 WL 22316555, at *4 (D. Minn. Oct. 6, 2003) ("Minnesota law . . . does not allow recovery for economic losses stemming from a

Minnesota courts recognize a special relationship only in a very narrow set of circumstances where the plaintiff's vulnerability and dependence or other public policy considerations require the imposition of special tort duties. *See Clark*, 552 N.W.2d at 709. The Minnesota Supreme Court has "carefully carved out" the following "as the outer boundaries" of special relationship categories: "common carriers, innkeepers, possessors of land who hold it open to the public, and persons who have custody of another person under circumstances in which that other person is deprived of normal opportunities of self-protection." *Id.*; *see also Johnson*, 553 N.W.2d at 49. Numerous decisions make clear that Minnesota courts are reluctant to extend special relationship duties beyond these categories. *See, e.g.*, *Funchess v. Cecil Newman Corp.*, 632 N.W.2d 666, 674 (Minn. 2001); *RKL Landholding*, 2013 WL 2149979, at *2–3 ("[T]he 'special relationship' exception is a narrow one . . . . The supreme court has expressed reluctance to expand on the exceptions to the general rule.").

Plainly, none of these traditional categories applies here. The Banks instead seek the creation of a new special relationship between merchants and issuing banks based on the allegation that the Banks "entrusted Target with the personal and financial information of customers using credit and debit cards issued by [the Banks] on the premise that Target would safeguard this information . . . ." Compl. ¶ 104. In addition to falling well outside the "outer boundaries" delineated by the Minnesota Supreme Court, the creation of an issuing-bank/merchant special relationship would undermine the role of

---

breach of an assumed duty."). The Banks do not allege any voluntary undertaking here, nor do they allege property damage or personal injury. Thus, the Banks' inability to allege a special relationship is fatal to their claim.

the Minnesota Legislature and otherwise be flatly inconsistent with prevailing Minnesota law.

To the extent the general rule in Minnesota is that a court should be reluctant to recognize new special relationship duties in tort, such reluctance surely must be amplified where the state legislature has already promulgated legislation on the topic that stops short of imposing by *statute* the very duty a plaintiff claims already exists at common law. Here, the Banks assert that the PCSA supports their negligence count. Compl. ¶ 110. In fact, however, that statute only serves to underscore the *non-existence* of the common-law tort duty on which that count is based.

Through the PCSA, the Legislature could have required merchants to reimburse issuing banks for costs associated with *any* data breach that the merchant allegedly could have prevented. It did not. Instead, the PCSA carefully limits the circumstances in which a merchant might be required to reimburse an issuing bank, imposing liability *only* when the data breach involved the theft of certain types of sensitive payment card data that the merchant had been storing in violation of the statute. Minn. Stat. § 325E.64, subd. 2–3 (2013). Here, the Banks' own allegations regarding the operation of the attacker's malware make clear that the PCSA provides the Banks no cause of action against Target. *See infra*, at Part IV.C. In asking this Court to find that Target owed them a *common-law* duty to take certain steps to prevent the Intrusion, then, the Banks are asking the Court to take the unprecedented step of imposing a common-law duty that goes above and beyond what the Legislature saw fit to impose. Target is not aware of any case in which a court found that a "special relationship" and accordingly a common-

law duty existed under Minnesota law in similar circumstances where the Minnesota Legislature had stopped short of statutorily imposing the duty in question. Courts in other data breach cases, however, have refused to create common-law duties beyond those enumerated by statute. *See Digital Fed. Credit Union v. Hannaford Bros. Co.*, No. BCD-CV-10-4, 2012 WL 1521479, at *3 & n.5 (Me. B.C.D. 2012) (rejecting issuing banks' attempts to impose "potentially unlimited liability" on merchants for a data breach, where the Maine Legislature limits a merchant's duty to notifying Maine residents of a breach); *Cooney v. Chi. Pub. Schs.*, 943 N.E.2d 23, 28–29 (Ill. App. Ct. 2010) (refusing to recognize a common-law duty to safeguard information where the Illinois Legislature requires only notice of a breach).

Even if the PCSA did not exist, this would not be an appropriate case for the Court to find that Target and the Banks had a "special relationship" such that Target had a common-law duty to protect the Banks from being injured by the criminal attack that *Target* suffered. As an initial matter, it does not appear that a Minnesota court ever has recognized a special relationship that requires one party to protect another from a third party's wrongful infliction of *economic* losses, as is alleged here. *See* Compl. ¶ 86. The distinction between third-party-inflicted economic losses on the one hand, and third-party-inflicted personal injury on the other, is consistent with the Minnesota Supreme Court's mandate that courts be reluctant to find new special relationships and has been noted in at least one decision as reason to reject claims of a special relationship. *See RKL Landholding*, 2013 WL 2149979, at *3 (no special relationship requiring contractor to protect owner's vacant building, in part because "there were no human occupants to

protect"). Moreover, even where grievous physical harm was alleged, Minnesota courts have found that policy considerations counsel against imposing tort duties requiring protection against criminal intruders. *See Funchess*, 632 N.W.2d at 673 n.4, 675 (finding no special relationship between landlord and tenant who was murdered by an intruder, reasoning that crime prevention is the duty of the government, not businesses, and noting the unpredictability of criminals "bent on defeating security measures").

But perhaps most significantly, Minnesota courts consistently and repeatedly have held that commercial transactions do not give rise to a special relationship, because commercial actors are "not the types of parties deemed to be vulnerable that would require protection." *See, e.g.*, *Superior Constr. Servs., Inc. v. Moore*, No. AO6-1491, 2007 WL 1816096, at *3 (Minn. Ct. App. June 26, 2007) (finding no special relationship between bank and a contractor, even though bank had custody and control of funds allegedly owed to contractor); *United Prods. Corp. of Am., Inc. v. Atlas Auto Parts, Inc.*, 529 N.W.2d 401, 403–04 (Minn. Ct. App. 1995) (finding no special relationship between neighboring businesses); *Mack v. Britto Cent., Inc.*, No. 13-197, 2013 U.S. Dist. LEXIS 110142, at *25 (D. Minn. Aug. 6, 2013) (dismissing negligence claim with prejudice where art dealer failed to plead a special relationship with artist and other art dealers), *superseded on other grounds*, 2014 WL 1608364 (D. Minn. Apr. 21, 2014).

Further, Minnesota courts are particularly unwilling to find a special relationship where, as here, a contractual scheme allocates (or could allocate) the parties' duties and risks. *See, e.g., RKL Landholding*, 2013 WL 2149979, at *3 (holding that if a property owner expected a contractor to protect the vacant building at issue, it "should have

obtained [contractor]'s agreement to do so."). This principle is not peculiar to claims of a special relationship, but rather has been recognized by the Minnesota Supreme Court as a fundamental boundary between duties in contract and tort. *See Glorvigen v. Cirrus Design Corp.*, 816 N.W.2d 572, 584 (Minn. 2012) (holding that a plaintiff cannot recover in negligence when its claims are premised on a defendant's allegedly having failed to comply with contractual duties); *see also M&I Marshall & Ilsley Bank v. Federated Mut. Ins. Co.*, No. 27-CV-10-15648, 2011 WL 2742950 (Minn. Dist. Ct. Feb. 2, 2011).

The Banks, as financial institutions that issue payment cards and participate in the complex networks required in order to process retail payment card transactions (Compl. ¶¶ 12, 17), are precisely the type of sophisticated commercial actors for which a special relationship will not be found, particularly since their negligence claim is premised on Target's allegedly having failed to comply with "industry standards and requirements," namely, the Card Operating Regulations and the PCI-DSS, which the Banks concede are enforceable on Target only as a result of Target's contracts with third parties. Compl. ¶¶ 18–19, 102; *see also* Compl. ¶¶ 17–18, 22, 106–07. The Card Operating Regulations, moreover, include specific remedies available to issuing banks in the event of a breach at a participating merchant, as the Banks no doubt are aware. *See* Visa International Operating Regulations, at *676 (Meal Decl., Ex. A) (describing process by which an issuing bank "may recover a portion of its Incremental Counterfeit Fraud losses and operating expenses resulting from an Account Data Compromise Event" if the merchant at issue had not been compliant with the PCI-DSS); MasterCard Security Rules and Procedures, Merchant Edition (August 30, 2013), at §10.2.5.3 (Meal Decl., Ex. B)

(describing reimbursement process enabling "an Issuer to partially recover costs" incurred in reissuing cards, enhanced monitoring of accounts, and counterfeit fraud losses); *see also In re TJX Cos. Retail Sec. Breach Litig.*, 246 F.R.D. 389, 398–99 (D. Mass. 2007) (describing methodology Visa enacted "to provide an efficient and cost-effective method of settling disputes arising out of account data compromises and resultant fraud"). Having acknowledged that the Card Operating Regulations govern members' participation in the card brand networks, the Banks cannot now seek to renegotiate these agreements and their remedies by asserting a claim in tort.

Finally, the allegations in the Complaint undermine the very assertion that *the Banks* "entrusted" anything to Target. *See* Compl. ¶ 104. The Banks repeatedly acknowledge that it was "the personal and financial information *of consumers*," not the Banks, that allegedly was stolen (Compl. ¶¶ 104–105, 107 (emphasis added)), and that this information was provided to Target *by such consumers* (Compl. ¶ 17). Thus, the Complaint does not even allege a direct relationship between the parties. Insofar as Minnesota courts already have rejected the claim that "a mere merchant-customer relationship" gives rise to a duty to protect customers, *Superior Constr.*, 2007 WL 1816096, at *3 (no special relationship between bank and contractor for whom it allegedly was holding funds in escrow), Target cannot be found to have a special relationship with the Banks, who are one more step removed. *Cf. Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 851–52 (N.D. Cal. 2012) (finding no special relationship under California law between Apple and Apple customers alleging that Apple failed to protect customers' information from third-party app developers).

Dismissal of the Banks' negligence claim because Target owed the Banks no duty is consistent with decisions dismissing similar claims asserted by issuing banks against merchants in other data breach cases. *See BancFirst v. Dixie Rests., Inc.*, No. CIV-11-174-L, 2012 WL 12879, at *4 (W.D. Okla. Jan. 4, 2012) (dismissing negligence claim under Oklahoma law against breached restaurant because there was no special relationship between the parties, noting the "attenuated" relationship between merchants and issuing banks and the fact that compliance with the PCI-DSS was a general obligation not owed to plaintiff in particular); *Digital Fed. Credit Union*, 2012 WL 1521479, at *3–4 (finding that breached grocery store owed no duty to issuing bank under Maine law, in part because the parties' risks were allocated in the Card Operating Regulations); *cf. Cumis Ins. Soc'y, Inc. v. Merrick Bank Corp.*, No. CIV 07-374-TUC-CKJ, 2008 WL 4277877, at *11–12 (D. Ariz. Sept. 18, 2008) (dismissing negligence claim asserted by insurer on behalf of issuing credit unions for failure to plead duty under Arizona law).[4]

[4] Target is aware of only one case in which a court has held that a merchant owed an issuing bank a common-law duty of care. *See Sovereign Bank v. BJ's Wholesale Club, Inc.*, 359 F. Supp. 2d 183, 193–95 (M.D. Pa. 2005). In that case, the negligence claim against the merchant was subsequently dismissed under the economic loss doctrine, 427 F. Supp. 2d 256, 534, and the ruling as to duty was thus never appealed. The decision is, in any event, inapposite for purposes of determining if the Banks have met their burden under Minnesota law, because the *Sovereign Bank* court did not require the plaintiff to plead a special relationship between itself and the defendant in order to survive dismissal. *See id.* Other courts, moreover, have expressly declined to follow the reasoning of the *Sovereign Bank* court. *See, e.g., Digital Fed. Credit Union*, 2012 WL 1521479 at *2–3 (rejecting issuing-bank arguments premised on the *Sovereign Bank* decision after noting that the Supreme Judicial Court of Maine, similar to the Minnesota Supreme Court, was "reticent to recognize new common law duties of care").

Courts similarly have recognized the lack of any duty in negligence between other members of the payment card networks. *See Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *18 (N.D. Ga. Feb. 5, 2013) (recommending dismissal where there was "no direct relationship" between cardholders and payment-card processor, and thus no duty in negligence, under Georgia law); *see also Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *9 (S.D.N.Y. June 25, 2010) (bank owed plaintiffs no duty under New York law relating to lost or stolen tapes containing plaintiffs' information, because plaintiffs' information was provided to the bank only through intermediaries, and, thus, the two had no "direct dealings"). Thus, dismissal of the Banks' claim for lack of duty not only is dictated by Minnesota law, but is consistent with the long line of dismissals in other jurisdictions.

2. *The Banks' Allegations of Breach of Duty Fail to Satisfy* Iqbal *and* Twombly.

Even if the Banks had alleged a duty of care, their allegations of negligent conduct are so conclusory as to fail to state a claim under *Iqbal* and *Twombly*.

The gravamen of the Banks' claim is that Target negligently failed to comply with "industry standards and requirements" – namely, the Card Operating Regulations and the PCI-DSS (Compl. ¶¶ 17–18, 22, 102, 106–07) – but that contention is contradicted by the allegations in the Complaint.[5]

[5] To the extent the Banks intended their negligence claim to be based in part on Target's alleged failure to comply with the PCSA, the Banks similarly have failed to plead any underlying violation. *See infra*, at Part IV.C.

The Banks allege that the Card Operating Regulations prohibit Target from "disclosing" payment card data, but it is undisputed that the Banks' claimed injuries resulted not from any disclosure by Target, but from a criminal intrusion in which data was stolen. *See, e.g.*, Compl. ¶¶ 14, 18.

With regard to the PCI-DSS, the Banks do not dispute that just two months before the Intrusion, an independent auditor certified that Target was compliant with "*all payment industry requirements*, including the [PCI-DSS]." Compl. ¶ 44. While the Banks allege various steps that Target might have taken to "foil" the "hacker's plan" (*see generally* Compl. ¶¶ 24–59), the Banks claim that just two of Target's alleged failures to act constituted PCI-DSS violations.[6] Specifically, the Banks allege that Target "could have" (1) "eliminate[ed] unneeded default accounts" and (2) "required vendors to more closely monitor the integrity of their critical file systems" as ostensibly "called for in the PCI-DSS 2.0." Compl. ¶ 52. However, neither purported PCI-DSS "requirement" actually appears in the laundry list of PCI-DSS requirements recited in the Complaint.

[6] For example, the Banks make numerous allegations that Target did not act on FireEye malware alerts in time to prevent the intrusion, but do not – and could not – allege that Target's FireEye-related actions violated the PCI-DSS. *See* Compl. ¶¶ 50–54. Moreover, as the Minnesota Supreme Court has recognized, allowing plaintiffs to proceed on allegations that "*further* security measures were required" because "existing security precautions [] failed" would provide defendants with "little idea [of] what is expected of him or her" and "discourage [defendants] from improving security." *Funchess*, 632 N.W.2d at 673 n.4, 675 (emphasis original). Indeed, the Banks admit that FireEye is a "state of art" malware detection tool used by the highest levels of the U.S. security infrastructure, that Target acquired it at a substantial cost in order to address increased cyber-attacks using new and sophisticated techniques, and that Target's rollout of the tool did not begin until June 2013. Compl. ¶¶ 29, 33–36. To penalize Target for alleged mistakes with respect to FireEye would impose precisely the perverse incentives *Funchess* sought to foreclose.

See Compl. ¶19 (alleging only that use of default *passwords* is prohibited and not referencing vendor security requirements). Further, the only network account referenced in the Complaint is the "limited network credentials" provided to Target's HVAC vendor (Compl. ¶ 38), which nowhere is alleged to be either unneeded or default. In short, the Banks have utterly failed to allege a violation of the industry standards for data security (i.e., the PCI-DSS) that Target supposedly had a common-law duty to satisfy. For this reason as well, then, their negligence count fails as a matter of law.

B. The Banks' Claim For Negligent Misrepresentation by Omission Must Also Be Dismissed.

The Complaint asserts as Count IV a claim for negligent misrepresentation by omission. To state a claim for negligent misrepresentation under Minnesota law, a plaintiff must plead that (1) defendant owed plaintiff a duty of care; (2) defendant supplied false information to plaintiff by either including therein a false affirmative representation or omitting therefrom information that renders the facts that are disclosed misleading; (3) plaintiff justifiably and detrimentally relied on the false information from the defendant; and (4) defendant failed to exercise reasonable care in communicating that information. *Noble Sys. Corp. v. Alorica Cent., LLC*, 543 F.3d 978, 985 (8th Cir. 2008); *Kichler v. Wells Fargo Bank, N.A.*, No. 12-1206 (JRT/AJB), 2013 WL 4050204, at *3 (D. Minn. Aug. 9, 2013) (citing *Williams v. Smith*, 820 N.W.2d 807, 815 (Minn. 2012)). Failure to plead any of these elements requires dismissal. *See, e.g.*, *Noble Sys. Corp.*, 543 F.3d at 984–86.

The Banks base their claim on Target's purported misleading omissions in (i) an unspecified "Privacy Policy," (ii) Target's alleged contract with an acquiring bank, in which Target purportedly agreed to comply with the Card Operating Regulations, (iii) an unspecified agreement in which Target allegedly agreed to comply with the PCI-DSS, and (iv) allegedly failing to communicate about the Intrusion in a timely manner. Compl. ¶¶ 18, 128–133. The Banks fail, however, to plead that Target owed them any duty of care in regard to these matters, that Target made any actionable misrepresentation by omission, or that the Banks actually relied upon any of the allegedly false information in question.

1. *The Banks Fail to Allege that Target Owed Them a Duty of Care.*

In the negligent misrepresentation context, "courts distinguish 'between a person engaged *in the business or profession of* supplying guidance to others and those engaged in commercial transactions at arm's length'" when determining if a defendant owed a plaintiff a duty. *Huntington Bancshares, Inc. v. Ally Fin., Inc.*, No. 27-CV-11-20276, 2012 WL 7749245, ¶ 39 (Minn. Dist. Ct. Dec. 11, 2012) (quoting *Safeco Ins. Co. of Am. v. Dain Bosworth, Inc.*, 531 N.W.2d 867, 871 (Minn. Ct. App. 1995)) (emphasis added). Unless a defendant is in the business of providing guidance to the plaintiff (e.g., an accountant-client, attorney-client, or guardian-ward relationship) – which, like in the negligence context, is referred to as a "special relationship," even though the tests are distinct – no duty is owed. *See Mack*, 2013 U.S. Dist. LEXIS 110142, at *18–22 (granting motion to dismiss for failure to plead duty because there was no special relationship between plaintiff and defendant artist and art dealers arising from sale of

paintings later discovered to be forgeries); *Woodcraft Indus., Inc. v. JBA Int'l, Inc.*, No. 01-373 DWF/RLE, 2001 WL 1640085, at *6 (D. Minn. June 14, 2001) (granting motion to dismiss for failure to plead duty where plaintiff alleged that it and defendant were businesses engaged in a transaction).

The Banks allege that Target is a retailer, not an adviser or fiduciary that is in the business or profession of guiding the Banks in their business transactions. Compl. ¶ 14. Further, Plaintiffs acknowledge that the parties are sophisticated business entities that interact with each other only indirectly (Compl. ¶¶ 7–12, 17–18), which occurs through the separate contracts that the Banks have with the Card Brands, that Target has with its acquiring bank, and that Target's acquiring bank in turn has with the Card Brands. *See supra*, at note 1. Indeed, since the Banks concededly are not parties to the alleged contract upon which they base much of their claim, in this case Target and the Banks had no commercial relationship whatever, much less a "special" one. And even if they did, that relationship would not differ one iota from the type of arm's length commercial relationship that Minnesota courts have routinely found *insufficient* for purposes of pleading duty in negligent misrepresentation cases. *See Huntington Bancshares*, 2012 WL 7749245, ¶¶ 40–41 (granting motion to dismiss for failure to plead duty where plaintiff alleged it was a consumer bank engaged in mortgage transactions with defendant financial institutions); *see also Regions Treatment Ctr., LLC v. New Stream Real Estate, LLC*, No. 13-1752 ADM/LIB, 2014 WL 107792, slip op. at *7 (D. Minn. Jan. 10, 2014) (denying motion for leave to amend complaint to add claim for negligent misrepresentation because plaintiff was a sophisticated business entity unable to plead

duty); *Woodcraft Indus., Inc.*, 2001 WL 1640085, at *6 (granting motion to dismiss on same grounds).

Even where a party is retained in a fiduciary or professional capacity to provide guidance with respect to a business transaction – which, again, the Banks fall well short of alleging – the resulting duty of care is owed only to those whom the information was intended to guide. *See Noble Sys. Corp.*, 543 F.3d at 985–86. Minnesota courts consistently have denied attempts to extend the duty to plaintiffs who were not parties to the contract at issue, or who were not retained by plaintiffs to provide such guidance. *See id.* (affirming grant of motion to dismiss where plaintiff was not a party to the contract at issue). For example, in *Safeco*, the Minnesota Court of Appeals held that even though the defendant-underwriter *was* in the business of supplying information for the guidance of its clients, the plaintiff-insurer was *not* defendant's client for purposes of the bond transaction at issue, and, thus, no duty of care was owed. *See Safeco*, 531 N.W.2d at 872; *see also Adams v. Rosensteel*, No. A13-0451, 2013 WL 6223562, at *3–5 (Minn. Ct. App. Dec. 2, 2013) (affirming grant of motion to dismiss because real estate broker owed a fiduciary duty only to his principal, the seller of a property, and not to plaintiff-buyers).

Here, the Banks' claim is premised on (i) an unspecified "Privacy Policy" (Compl. ¶ 128), which is not alleged to have been directed to the Banks specifically or even financial intuitions generally, (ii) an agreement between Target and its acquiring bank (Compl. ¶¶ 18, 129), which the Banks do not allege to have ever even seen, much less to have been the intended beneficiaries of, (iii) an unspecified agreement in which Target allegedly agreed to comply with the PCI-DSS, which again the Banks do not claim to

have been a party to or an intended third-party beneficiary of, and (iv) Target's alleged failure to timely communicate information to unspecified persons or entities concerning the Intrusion (Compl. ¶ 134). Because the Banks have not alleged that they were the intended recipient of any of the allegedly false information in question, they would have failed to plead that Target owed *them* a duty of care in generating that information even if they had a plausible basis to allege that Target generated that information in the capacity of a business providing guidance to *someone else* (as noted above, no such basis exists).

Dismissal of the Banks' negligent misrepresentation claim for failure to plead duty is also consistent with decisions reached in other data breach cases involving similar allegations. In *Cumis Insurance Society*, 2008 WL 4277877, for example, the court dismissed claims based on alleged misrepresentations about defendants' compliance with the Card Operating Regulations, because the plaintiff insurance company did not allege that the defendant made any representations to plaintiff or its insureds (issuing banks) distinct from representations made to all participants in the Visa and MasterCard payment systems. *Id.* at *11–12.

In cases premised on a defendant's alleged failure to promptly inform third parties of an intrusion, courts have routinely found that no legal duties or remedies exist beyond those imposed by statute. *See In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 124–25 (D. Me. 2009) (dismissing negligent misrepresentation by omission claim based on defendants' alleged failure to notify plaintiffs of an intrusion where the state's "detailed" data breach notification statute left the court "wary of creating any new state standards where the Maine Law Court has not

already clearly provided a remedy"), *aff'd in part and rev'd in part sub nom Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011); *see also Willingham*, 2013 WL 440702, at *18 (recommending dismissal where state statute did not require defendant to notify plaintiffs). In Minnesota, the data breach notification law does not require any notification to issuing banks. *See* Minn. Stat. § 325E.61(a) (2013). Thus, the Banks' allegations seek not only the creation of a new common-law duty, but one that subverts the clear limitations imposed by the Minnesota Legislature.

2. *The Banks Fail to Allege Any Actionable Misrepresentation by Omission.*

The Banks also fail to allege any actionable misrepresentation by omission. It is well-established that claims for negligent misrepresentation and omission are subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). *See, e.g.*, *Trooien v. Mansour*, 608 F.3d 1020, 1028 (8th Cir. 2010) (negligent misrepresentation is "an allegation of fraud which must be pled with particularity"). Rule 9(b) requires a plaintiff to state claims with particularity, and to accompany such claims with "the who, what, where, when, and how" of the alleged deception. *Sneh v. Bank of N.Y. Mellon*, Civ. No. 12 -954 (MJD/JSM), 2012 WL 5519690, at *7 (D. Minn. Oct. 30, 2012), *adopted by* 2012 WL 5519682 (D. Minn. Nov. 14, 2012) (quoting *BJC Health Sys. v. Columbia Cas. Co.*, 478 F.3d 908, 917 (8th Cir. 2007)); *see also Cox v. Mortg. Elec. Registration Sys.*, 685 F.3d 663, 673 (8th Cir. 2012) (holding that plaintiffs "must plead the time, place, and contents of" false representations, as well as the identity of the party making them); *In re Digi Int'l Inc. Sec. Litig.*, 6 F. Supp. 2d 1089, 1104 (D. Minn. 1998).

The Complaint points to two sets of purportedly deceptive representations regarding Target's information security, neither of which is adequately pled. First, the Banks cite an unspecified "Privacy Policy" and "other actions and representations" in which Target allegedly "held itself out to the Banks and the FI Class" as having security measures "sufficient to protect" shoppers' information. Compl. ¶ 128. But the Complaint fails to provide even basic facts about the "Privacy Policy": when it was issued, the statements made therein through which Target allegedly "held itself out" to the Banks, the specific information Target purportedly omitted, or how any such statements were directed to the Banks for guidance in their business transactions. The Complaint similarly provides no detail whatsoever regarding the alleged "other actions and representations." Conclusory allegations such as these fail to meet even Rule 8 pleading standards, much less the heightened requirements of Rule 9(b). *Cf. Riley v. Cordis Corp.*, 625 F. Supp. 2d 769, 786–87 (D. Minn. 2009) (granting motion to dismiss even though plaintiff "describe[d] the contents, as well as the time and place" of some alleged misrepresentations but did "not allege[], with specificity, who made the representations, when the representations were made, [or] to whom the representations were made").

Second, the Banks allege that Target "agree[d] to comply with both Card Operating Regulations and the PCI-DSS" when it purportedly "knew or should have known that it was not in compliance" with them. Compl. ¶¶ 129–30. The Complaint, again, fails to set forth basic facts about the purported representations, such as the identify of the acquiring bank(s) or other third party with which Target purportedly

contracted, when the alleged agreement(s) were executed, the terms of any such agreements, the specific information allegedly omitted, and when and how the agreements' terms were directed to the Banks. *See* Compl. ¶¶ 18, 129–30. Moreover, the Banks fail to plead any violation of either the Card Operating Regulations or the PCI-DSS, much less with the particularity required by Rule 9(b). *See supra*, at Part IV.A.2.

Even if the Banks had satisfied Rule 9(b), their negligent misrepresentation claim would still fail to allege an actionable misrepresentation. In dismissing claims for negligent misrepresentation, this Court previously has recognized that "it is not possible to be negligent in failing to ascertain the truth or falsity of one's present intention to act in the future." *See Mitchell v. Franklin Bank, S.S.B.*, No. Civ. 05-1320 PAMRLE, 2005 WL 2406034, at *3 (D. Minn. Sept. 29, 2005) (dismissing claim premised on defendant's purported negligent misrepresentations about its intent to comply with federal law and pay operating expenses). Thus, any assertion that Target negligently represented its intent to maintain security measures "sufficient to protect" shoppers' information or to comply with Card Operating Regulations or the PCI-DSS fails as a matter of law. *See* Compl. ¶ 128. Minnesota courts, moreover, consistently have found that negligent misrepresentation claims premised on contractual provisions are not actionable, holding that to allow otherwise would contravene the law of contracts. *See, e.g.*, *Safeco*, 531 N.W.2d at 871; *Woodcraft Indus., Inc.*, 2001 WL 1640085, at *6.

Notably, courts in other data breach cases have explicitly rejected the very argument that the Banks assert here. *See, e.g.*, *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 594–96 (S.D. Tex. 2011)

(granting motion to dismiss issuing banks' claim that a payment processor negligently misrepresented its compliance with the Card Operating Regulations, because the Regulations themselves "provide compensation if circumstances later prove that representation false" and because plaintiffs did not allege that defendant never intended to comply with them), *rev'd on other grounds*, 729 F.3d 421 (5th Cir. 2013); *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club*, 918 N.E.2d 36, 49 (Mass. 2009) (affirming summary judgment for breached retailer on negligent misrepresentation claim because "failure to perform a contractual duty [to comply with the Card Operating Regulations] does not give rise to a tort claim for negligent misrepresentation" and because there was no evidence that defendants did not intend to comply with Card Operating Regulations when they entered the contract).

As to the Banks' allegation that Target "failed to timely communicate information concerning the data breach" (Compl. ¶ 133), that assertion on its face cannot be the basis for a negligent misrepresentation claim, for it concerns only the timeliness of Target's communications, and not whether the content of any such communication was false. *See Kichler*, 2013 WL 4050204, at *3 (negligent misrepresentation requires false information through either "an affirmative statement that is itself false or" "concealing or not disclosing certain facts that render the facts that are disclosed misleading."). Moreover, the assertion simply is not plausible, given that Target's notice was provided within four

days of confirming the Intrusion.[7] *See* Compl. ¶ 68 n.2. Thus, no actionable misrepresentation by omission is alleged in that regard either.

3. *The Banks Have Failed to Allege Reliance.*

Even if the Banks had alleged a duty and an actionable misrepresentation by omission, Count IV is nonetheless defective because the Banks fail to allege reliance.

In order to state a negligent misrepresentation claim under Minnesota law, a plaintiff must allege that it actually read and relied upon the misrepresentations or omissions alleged, setting forth specifically how and why their reliance caused them harm. *See In re Digi*, 6 F. Supp. 2d at 1104 (granting motion to dismiss where plaintiff alleged only that it "directly or constructively relied on" the alleged statements and omissions at issue). These allegations must be pled with particularity under Rule 9(b); conclusory allegations of reliance do not suffice. *Cox*, 685 F.3d at 672–74 (affirming grant of motion to dismiss where plaintiffs failed to allege how reliance on particular representations proximately caused their home foreclosure).

Here, the Complaint is devoid of any allegation as to reliance on any of the alleged misrepresentations, even a conclusory one. No Plaintiff alleges that it read the "Privacy Policy," the alleged agreement between Target and its acquiring bank, the unspecified agreement in which Target allegedly agreed to comply with the PCI-DSS, or any other

[7] Minnesota's data breach notification statute (which, as noted above, does not require notice to the Banks) does not specify an amount of time that constitutes "unreasonable delay." *See* Minn. Stat. § 325E.61(a). All of the state data breach notification statutes that do so specify, however, indicate that 4 days is more than reasonable. Fla. Stat. § 817.5681(1)(a) (allowing 45 days following discovery); Ohio Rev. Code § 1349.19(B)(1) (same); Wis. Stat. § 134.98(3)(a) (same); *cf.* Me. Rev. Stat. tit. 10, § 1348(3) (allowing 7 days after law enforcement approval).

document in which the allegedly false information supposedly generated by Target allegedly may have appeared, and no Plaintiff alleges that it undertook or refrained from undertaking any particular action in detrimental reliance upon the allegedly false information contained within those documents or as a result of Target's alleged failure to timely communicate information about the Intrusion. *See, e.g.*, *Raden v. BAC Home Loans Servicing, LP*, No. 12-CV-1240 (PJS/TNL), 2013 WL 656624, at *4–5 (D. Minn. Feb. 22, 2013) (granting motion to dismiss where plaintiffs did not plead with particularity what "loss-mitigation options" they would have successfully pursued and how, absent reliance on defendant's misrepresentation); *see also Heartland*, 834 F. Supp. 2d at 594 (finding reliance not adequately pled in data breach case where plaintiffs did not allege "that any representations by the defendants induced them to become or remain issuers in the Visa and MasterCard system, or that they have withdrawn from or altered their participation in the system after becoming aware of the defendants' breach") (quoting *Cumis Ins. Soc'y, Inc.*, 918 N.E.2d at 49).

C. The Banks' Claim For Violation of the Minnesota Plastic Card Security Act Must Be Dismissed.

1. *The Banks Fail to Allege that Target Retained Any Payment Card Data in Violation of the Minnesota Plastic Card Security Act.*

The Banks' own allegations rebut their claim in Count Two that Target violated the PCSA. The PCSA prohibits merchants "conducting business in Minnesota" from retaining three types – and only three types – of payment card data after a transaction has been authorized: (1) card security code data, (2) PIN verification code numbers, and (3)

the full contents of any track of magnetic stripe data.[8] Minn. Stat. § 325E.64, subd. 2. If a merchant violates the PCSA and the impermissibly stored data is "affected by [a data] breach," the PCSA provides that the merchant must reimburse issuing banks that issued affected cards for "the costs of reasonable actions undertaken by the financial institution as a result." *Id.* at subd. 3.

Tracking the text of the statute, the Banks allege that Target violated the PCSA "by retaining the card security code data, the PIN verification code number, and/or the full contents of Target customers' magnetic stripe data," and that they "suffered injury" as "a direct and proximate result of Target's violation." Compl. ¶¶ 118, 120. The Banks allege nothing whatsoever in support of their conclusory claim that Target stored PIN verification code numbers or full magnetic stripe data post-authorization, much less that any such stored data was affected by the Intrusion. As for card security codes, the *only* "fact" that the Banks allege is that an analyst with no connection to Target speculated that "[t]he fact that three-digit CVV security codes were compromised shows they were being stored."[9] Compl. ¶ 82. The Banks' own allegations, however, highlight the flaw in that

[8] The Banks allege that the PCSA bars storage of all in-scope data types only if stored for more than 48 hours after authorization. Compl. ¶ 114. The 48-hour provision, in fact, only applies to PIN debit transactions. Minn. Stat. § 325E.64, subd. 2. This distinction, however, is immaterial here because the Banks do not plausibly allege that Target stored *any* of the three data types for *any* period of time, much less 48 hours post-authorization.

[9] The Banks' other allegations regarding customer data storage do not involve the types of data that the PCSA covers. The Banks' allegation that Target "improperly retained *customer data* (potentially for many months)" was based on Target's announcement that the Intrusion involved "names, mailing address, phone numbers, and email address." Compl. ¶ 75 (emphasis added). None of these data types is in-scope for the PCSA. Minn. Stat. § 325E.64, subd. 2. The Banks' allegation that Target stored "full [payment card] account number[s]" along with "the expiration date and the cardholder's name," Compl.

analyst's logic and why their PCSA claim must be dismissed: cyber criminals are fully capable of stealing payment card data that was never stored by a merchant for future use, and that is exactly what occurred here.

As the Banks acknowledge, the criminal intruders' point-of-sale malware was designed to steal payment card data "***in real time***" – not after the transaction had been authorized – "each time customers swiped their card at a Target store."[10] Compl. ¶ 56 (emphasis added). As the Complaint describes it, the malware

> ***actively*** collect[ed] card records ***from live customer transactions***. The way the malware worked was simple: when a customer went to any in-store Target cash register to pay for an item and swiped his or her card, the malware stepped in and captured the shopper's card number and other sensitive financial information.

Compl. ¶ 49 (emphasis added). The Banks' description of the Intrusion, moreover, nowhere suggests that the intruders used any mechanism other than the point-of-sale malware described above to capture the allegedly stolen payment card data that underlies all of the Banks' alleged injuries. *See* Compl. ¶¶ 47–67. The Banks' allegation that Visa had previously issued reports "alerting Target to attacks using RAM scraper malware, or

---

¶ 82, is similarly irrelevant for purposes of determining if Target violated the PCSA because the "*full* magnetic stripe data" that cannot be stored under the PCSA is composed of name, card number, expiration date *and* a security code, such as a CVV. *Cf.* Compl. ¶ 71 (describing the elements of "full magnetic stripe data"). Nowhere, moreover, do the Banks allege that the particular payment card data referenced in Paragraph 82 was affected by the Intrusion.

[10] The Banks allege that *after* the "real-time" data capture, "*the hackers* temporarily stored the data" in staging points on Target's network for six days before exfiltrating it. Compl. ¶ 56 (emphasis added). Even if this were true, it would not salvage the Banks' PCSA claim, since the PCSA only addresses data storage by a merchant or by a merchant's service provider. Minn. Stat. § 325E.64, subd. 2.

memory parsing software, which enables cyber criminals to grab encrypted data by ***capturing it when it travels through the live memory of a computer***," Compl. ¶ 30, underscores that the simple fact that payment card data is stolen does not mean that the merchant at issue has been storing it, as the analyst asserted.

The Banks' claim is, therefore, particularly ripe for dismissal since they not only failed to plead facts to support Target's alleged violation of the PCSA, but actually pleaded facts that "would appear to refute any such conclusion." *Clark v. Northland Grp., Inc.*, No. 14-606 (PAM/JJG), 2014 WL 3828218, slip op. at 3 (D. Minn. Aug. 4, 2014); *see also Lubbers v. Deutsche Bank Nat. Trust Co.*, No. 13-926 (DWF/JSM), 2013 WL 6729004, slip op. at 12 (D. Minn. Dec. 19, 2013) (granting motion to dismiss where exhibits to the complaint where "in direct contradiction to plaintiff's factually devoid assertions"). Since the only "fact" supporting the Banks' allegation of a PCSA violation – an analyst's opinion – is undercut by the Banks' own description of how the Intrusion occurred, the Banks are left with nothing more than "a formulaic recitation of the elements of a cause of action" that cannot survive a motion to dismiss. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

2. *The Minnesota Plastic Card Security Act Only Applies to Business Conducted in Minnesota.*

The PCSA only applies when an entity is "conducting business in Minnesota [and] accepts an access device in connection with a transaction." Minn. Stat. § 325E.64, subd. 2. Accordingly, even if the Banks had pled facts sufficient to state a claim under the PCSA – as set forth above, they have not – their PCSA claim should still be dismissed to

the extent it is based on underlying customer transactions that occurred in states other than Minnesota.[11]

D. Because the Banks Have Failed to State a Claim For Violation of the Minnesota Plastic Card Security Act, They Have Likewise Failed to State a Claim For Negligence *Per Se* Based on that Act.

In Minnesota, certain statutory violations can substitute for the duty and breach elements of a claim for ordinary negligence, converting it to a negligence *per se* claim. *Mervin v. Magney Constr. Co.*, 399 N.W.2d 579, 582 (Minn. Ct. App. 1987). The Banks in Count Three assert that Target's "violation of the [PCSA] constitutes negligence *per se*." Compl. ¶ 126. As discussed above, however, the Banks have failed to plead a violation of the underlying statute and thus have failed to plead a breach of duty. The negligence *per se* claim therefore necessarily fails. *Yang Mee Thao-Xiong v. Am. Mortg. Corp.*, No. 13-CV-354 (MJD/TNL), 2013 WL 3788799, slip op. at 2 (D. Minn. July 18, 2013) (dismissing negligence *per se* claim where the plaintiffs' amended complaint itself confirmed that no underlying statutory violation had occurred).

V. CONCLUSION

For the foregoing reasons, Target respectfully requests that the Court grant Target's motion to dismiss the Complaint in its entirety.

[11] Notably, an interpretation of the PCSA as applicable to transactions in stores outside Minnesota with non-Minnesota shoppers would require dismissal of the Banks' entire PCSA claim, since it would impose conditions on "commerce occurring entirely outside the boundaries of" Minnesota and, therefore, violate the "dormant" component of the Commerce Clause of the U.S. Constitution. *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989); *see also Cotto Waxo Co. v. Williams*, 46 F.3d 790, 793 (8th Cir. 1995) ("Extraterritorial reach invalidates a state statute when the statute requires people or businesses to conduct their out-of-state commerce in a certain way.").

Respectfully submitted,

Date: September 2, 2014

/s/ Wendy J. Wildung

Wendy J. Wildung, #117055
Michael A. Ponto, #203944
FAEGRE BAKER DANIELS LLP
2200 Wells Fargo Center
90 South Seventh Street
Minneapolis, MN 55402-3901
P: (612) 766-7000
F: (612) 766-1600 (Facsimile)
wendy.wildung@faegrebd.com
michael.ponto@faegrebd.com

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
P: (617) 951-7000
F: (617) 951-7050
Douglas.Meal@ropesgray.com

Michelle Visser
ROPES & GRAY LLP
Three Embarcadero Center
San Francisco, CA 94111-4006
P: (415) 315-6300
F: (415) 315-6350
Michelle.Visser@ropesgray.com

Attorneys for Defendant Target Corporation

US.54791500.01

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

LR 7.1(f) & LR 72.2(d)
CERTIFICATE OF COMPLIANCE

In re: Target Corporation Customer Data Security Breach Litigation

This Document Relates to:
All Financial Institution Cases

Case Number: MDL No. 14-2522 (PAM/JJK)

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,

vs.

Target Corporation,

Defendant.

I, Douglas H. Meal, certify that the

☒ Memorandum titled: Defendant's Memorandum Of Law In Support Of Motion To Dismiss the Consolidated Class Action Complaint complies with Local Rule 7.1(f).

or

€ Objection or Response to the Magistrate Judge's Ruling complies with Local Rule 72.2(d).

I further certify that, in preparation of the above document, I:

☒ Used the following word processing program and version: Microsoft Word 2010, and that this word processing program has been applied specifically to

include all text, including headings, footnotes, and quotations in the following word count.

or

€ Counted the words in the document.

I further certify that the above document contains the following number of words: 8,856.

Date: September 2, 2014

s/ Wendy J. Wildung

Wendy J. Wildung, #117055
Michael A. Ponto, #203944
FAEGRE BAKER DANIELS LLP
2200 Wells Fargo Center
90 South Seventh Street
Minneapolis, MN 55402-3901
P: (612) 766-7000
F: (612) 766-1600 (Facsimile)
wendy.wildung@faegrebd.com
michael.ponto@faegrebd.com

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
P: (617) 951-7000
F: (617) 951-7050
Douglas.Meal@ropesgray.com

Michelle Visser
ROPES & GRAY LLP
Three Embarcadero Center
San Francisco, CA 94111-4006
P: (415) 315-6300
F: (415) 315-6350
Michelle.Visser@ropesgray.com

Attorneys for Defendant Target Corporation