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 REPLY TO PLAINTIFFS' OPPOSITION TO THE MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

In an effort to avoid dismissal of each count in their Complaint, the Banks resort to "facts" not alleged in the Complaint and "legal standards" not part of Minnesota law.

I. ARGUMENT

A. The Banks Fail to Allege a PCSA Violation.

The parties agree that the PCSA only prohibits "businesses like Target" from "retaining" three types of payment card data: CVV codes, PIN values, and full-track data ("Protected Data"). Opp'n at 9. While the Banks *argue* that Target had a policy of retaining Protected Data, their Complaint contains no such allegations. *See Five Smiths, Inc. v. Nat'l Football League Players Ass'n*, 788 F. Supp. 1042, 1050 (D. Minn. 1992) ("[A] complaint may not be amended by the briefs in opposition to a motion to dismiss."). The allegations they cite – save the analyst's speculation in Paragraph 82 – all involve data types that do *not* qualify as Protected Data. *See* ECF. No. 185 ("Mem.") at 27 n.9. As for the analyst's theory that CVV codes *only* can be stolen if a retailer previously had stored them, the Banks make no attempt to address their own allegations' refutation of the analyst's baseless conjecture. Mem. at 27–29.

The Banks try to salvage their claim by proposing an illogical reading of the PCSA that would render *Target* liable for the *criminal intruders'* alleged acts. Relying on a single dictionary definition, the Banks argue that a retailer "retains" Protected Data in violation of the PCSA if "*hackers* temporarily store[] the data" (Compl. ¶ 56 (emphasis added)) on the retailer's network.[1] Opp'n at 12. Other definitions of "retain," however,

[1] Under the Banks' untenable theory, a retailer would be strictly liable under the PCSA if there was any post-authorization delay – even a millisecond – between the time criminals

provide that intent to keep the data for future use is required. *See, e.g.*, *Cambridge Business English Dictionary*, http://dictionary.cambridge.org/us/dictionary/business-english/retain ("to keep a record, document, etc. that might be needed in the future"). More importantly, the very case the Banks cite for their "plain language" argument clarifies that "technical words and phrases [must] be given their special or defined meaning." *In re Welfare of J.J.P.*, 821 N.W.2d 260, 266 (Minn. 2013); *see also* Minn. Stat. § 645.08(1). "Data retention" – the focus of the PCSA – is a technical term. It means the *storage* of data *for future usage*. *See Computer Desktop Encyclopedia*, http://lookup.computerlanguage.com/host_app/search?cid=C999999&term=data+retention&lookup.x=0&lookup.y=0 ("storing data for backup and historical purposes"); *TechTarget Storage Media*, http://searchstorage.techtarget.com/definition/data-retention ("the continued storage of an organization's data for compliance or business reasons"). Canons of statutory construction, therefore, dictate that a retailer only "retains" Protected Data under the PCSA if it affirmatively stores Protected Data for its own future use – facts not alleged here.

While there is, therefore, no need for the Court to examine the legislative history of the PCSA before dismissing the Banks' PSCA claim,[2] it would reach the same result if it did. The legislative history confirms the PCSA was enacted to incentivize retailers to

---

intercepted "live" CVV codes or full-track data and the time they exfiltrated it from a retailer's network (i.e., in nearly every payment card breach *not* involving theft of previously stored data).

[2] Contrary to the Banks' assertions, whether a criminal's temporary storage of Protected Data on a retailer's network violates the PCSA is a legal issue appropriately decided on a motion to dismiss.

stop storing Protected Data "in their computer databases," because such data "can fall into the wrong hands." Press Release, Office of State Sen. Mary A. Olson, Senate Approves Minnesota Plastic Card Security Act (May 15, 2007), http://www.senate.mn/members/member_pr_display.php?ls=86&id=925. It further confirms retailers can *only* be liable "if they are found to have improperly *stored*" Protected Data. *Id.* (emphasis added). Notably, the dictionary the Banks rely upon for their "plain language" argument defines the verb "store" synonymously with the technical definition of "data retention," to mean "[k]eep or accumulate (something) *for future use*." *Oxford English Dictionary* (online ed.), http://www.oxforddictionaries.com/us/definition/american_english/store (emphasis added).[3]

B. <u>The Banks Fail to Allege Negligence *Per Se*.</u>

The parties agree that a violation of an underlying statute is a necessary element of negligence *per se*. Because the Banks failed to plead a PCSA violation, they have likewise failed to plead negligence *per se*.

C. <u>The Banks Fail to Allege Negligence.</u>

1. *No Duty.*

The Banks admit their claim's premise is that Target "fail[ed] to protect" them against harm resulting from the actions of sophisticated criminal hackers. Opp'n at 18 (alleging Target failed to prevent and failed to halt the Intrusion). It is well-established

[3] The Court thus need not address the Banks' assertion that the PCSA applies to transactions occurring outside Minnesota, but Target stands by its position to the contrary. *See* Mem. at 29–30.

that Minnesota employs a distinct "special relationship" test for allegations of a failure to protect another from third-party harm. *See* Mem. at 6; *Domagala v. Rolland*, 805 N.W.2d 12, 23 (Minn. 2011) (rule "comprises a legal doctrine separate and distinct from other forms of negligence"). The Banks cite no case to the contrary,[4] yet spend much of their brief arguing they have pled a duty under Minnesota's inapplicable general negligence standard.[5]

The Banks' resort to the general negligence standard only underscores their failure, and inability, to plead a special relationship. The Banks do not – and cannot – argue that the merchant/issuer relationship is among those recognized as "special" under Minnesota law,[6] and each of their theories for why they have nonetheless alleged a special relationship is contradicted by Minnesota law.

---

[4] None of the cases cited by the Banks in their general negligence analysis applies Minnesota's general negligence standard to allegations of a duty to protect against third-party harm. The data breach cases they rely upon did not involve Minnesota law and are, therefore, inapposite as to what standard applies here.

[5] Although the general negligence factors are inapplicable, they too weigh against the Banks: (1) none of the alleged failures by Target to prevent and stop the unprecedented Intrusion rendered it (much less the Banks' alleged injury) foreseeable; (2) the connection between Target's conduct and the Banks' alleged injury is indirect (Compl. ¶¶ 17, 56, 104–05, 107 (the information allegedly belongs to consumers and was stolen by criminals)); (3) any moral blame belongs to the criminal hackers; (4) and (5) Minnesota has a policy against imposing tort duties for protection against criminal harm, *e.g.*, *Funchess v. Cecil Newman Corp.* 632 N.W.2d 666, 673–75 (Minn. 2004), the rights and burdens with respect to the security of payment card data are comprehensively allocated by contract, *see* Mem. at 11–12, and the Minnesota Legislature could have extended liability under the PCSA to any "failures" to prevent intrusions, but did not, *infra* at 7.

[6] The Banks urge that the land possessor/invitee category is "instructive," but do not allege such a relationship here. Even if Minnesota law encouraged courts to find new special relationships by analogy – it does not, *see Clark ex. Rel. H.B. v. Whittemore*, 552 N.W.2d 705, 707 (Minn. 1996) (traditional categories are "outer boundaries" of special

First, the Banks *argue*, but nowhere allege, that they were "particularly vulnerable and dependent on [Target]" and that "only Target was in a position to stop the Breach." Opp'n at 29–30. But even if the Banks had pled that Target was the only industry stakeholder able to protect them – which Target disputes – such allegations would not suffice. *See Johnson v. State*, 553 N.W.2d 40, 49 (Minn. 1996) (no duty to protect even where action "is necessary for another's aid or protection"). Minnesota law, moreover, deems enterprises such as the Banks capable of protecting themselves. *See Superior Constr. Servs., Inc. v. Moore*, No. A06-14912, 2007 WL 1816096, at *3 (Minn. Ct. App. June 26, 2007). The Banks' cited cases – which variously allege child abuse (*Becker v. Mayo Foundation*), rape (*Erickson v. Curtis Investment Co.*), suicide (*Donaldson v. Young Women's Christian Association of Duluth*), severe brain damage (*Tiedeman ex rel. Tiedeman v. Morgan*), and physical battery (*Errico v. Southland Corp.*) – underscore that sophisticated commercial actors alleging *only* economic harm[7] are *not* "particularly vulnerable" plaintiffs for whom special relationship duties might be recognized.[8]

---

relationship) – the Banks' cases support no analogous duty. *See Errico v. Southland Corp.*, 509 N.W.2d 585, 588 (Minn. Ct. App. 1993) (possessor of land's duty *to customers* limited to property's physical condition, "not . . . criminal acts of independent third persons").

[7] The Banks' assertion that "physical replacement of cards" constitutes property damage has been roundly rejected. *See, e.g., In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009); *Pa. State Emps. Credit Union v. Fifth Third Bank*, 398 F. Supp. 2d 317, 330 (M.D. Pa. 2005).

[8] The Banks do not dispute that no court has found a special relationship when the alleged loss was merely economic, and they are incorrect that type of harm is irrelevant. *See RKL Landholding v. James*, No. A12-1739, 2013 WL 2149979, at *3 (Minn. Ct. App. May 20, 2013). The Banks' reliance on *Erickson* for the assertion that special

Indeed, the Banks *did* secure a potential contractual remedy for the types of losses they allege, confirming that they are not "particularly vulnerable" plaintiffs. *See* Compl. ¶ 17; Mem. at 9, 11–12; *cf. Digital Fed. Credit Union v. Hannaford Bros. Co.*, No. BCD-CV-10-4, 2012 WL 152149, at *3 (Me. B.C.D. Mar. 14, 2012) (issuers manage risks of merchant-breaches through contracts, such that tort duty is unnecessary).[9] The Banks' assertion that Target's acquirer would pay any contractual recovery in the first instance is irrelevant to whether a contractual regime exists to address the types of losses the Banks allege here. *See* Mem. at 11–12, Meal Decl. Ex. A, at *679, *681 and Ex. B, at §§10.2.5.3–10.2.5.5 (making clear that acquirers' potential liability extends to intrusions suffered by their merchants).

In addition, the Banks admit that being vulnerable is not enough; a plaintiff must have entrusted its safety to the defendant and the defendant must have accepted that responsibility. *See* Opp'n at 32. The Complaint nowhere alleges that the Banks entrusted *anything* to Target, much less their safety, or that Target accepted such responsibility.

Second, the Banks assert that the harm they allegedly suffered was foreseeable, but foreseeability is a separate requirement not relevant to the special relationship inquiry. *See* Mem. at 6.

---

relationships can exist in the commercial context is particularly misplaced, as the plaintiff there was a woman who was raped in a parking facility.

[9] The Banks argue that "the [Card Operating] Regulations themselves nowhere limit a card-issuing bank's common law remedies." Opp'n at 36. *Minnesota law*, however, prohibits the Banks from recovering in negligence for claims premised on contractual duties, no matter who the parties to the contract are. *See* Mem. at 10–11. The cases cited by the Banks (none of which analyzes whether a special relationship exists) nowhere hold otherwise.

Third, the Banks argue that the PCSA supports finding that Target owed them a common-law duty. However, courts must be "especially reluctant" to impose a common-law duty that goes above and beyond whatever duty the legislature saw fit to impose by statute. *Dukowitz v. Hannon Sec. Servs.* 841 N.W.2d 147, 153 n.3 (Minn. 2014). The *Hannaford* decision cited by the Banks states the same. *See* Mem. at 8–9. Because the Legislature has "addressed the general area of policy at issue" and has strictly limited retailers' liability to issuers in the data-breach context as set forth in the PCSA, the Banks' negligence claim is a "mere[] attempt to make an end-run around the statute" that the Court should reject. *Weigman v. Everest Inst.*, 957 F. Supp. 2d 1102, 1109-10 (D. Minn. 2013).

Fourth, the Banks assert that Target "voluntarily assumed" a duty, but admit this exception only applies in cases involving personal injury or property damage, which are not alleged here. *See* Opp'n at 34. Additionally, their attempt to distinguish *Funchess* is unavailing. Like the landlord there, the Complaint does not allege Target undertook any actions specifically for the Banks' benefit. 632 N.W.2d at 675.

Finally, the Banks erroneously contend that "[f]inancial institutions' common law rights against merchants . . . are confirmed by other data breach cases." Opp'n at 36. In actuality, courts repeatedly have dismissed on the pleadings banks' negligence claims in the data-breach context. *See* Mem. at 13–14. Notably, the Banks completely ignore the only opinion decided under the "special relationship" test applicable here. *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 because no special relationship existed between merchants

and issuers). Indeed, to Target's knowledge, *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d. 183 (M.D. Pa. 2005), is the *only* data breach decision holding that a merchant owed an issuer a common-law duty, and it is inapposite. *See* Mem. at 13 n.4. The Banks also mischaracterize *Lone Star National Bank N.A. v. Heartland Payment Systems*, 729 F.3d 421, 426–27 (5th Cir. 2013) as finding a duty. In *Heartland*, the court held *only* that New Jersey's economic loss doctrine could not be found applicable at the motion to dismiss stage. *Id.* at 427. Thus, while the *Heartland* court did comment in dicta that a processor "may" have a negligence-based duty of care to issuers, *id.* at 426, the court ultimately remanded that and all other unreached issues to be decided in the first instance by the district court, *id.* at 427, where they are currently being briefed to Judge Rosenthal. *See* No. 09-md-02046 (S.D. Tex.).[10]

2. *No Breach of Duty.*

The mere *fact* of a sophisticated criminal intrusion does not imply negligence. As to the gravamen of the Banks' claim – that Target "failed to adhere to applicable industry [security] standards" (Opp'n at 27) – the Banks admit Target was certified as compliant with "all 'payment industry requirements,' including the [PCI-DSS]" (Compl. ¶ 44), and offer no rejoinder to Target's argument that the Banks have not adequately pled any PCI-DSS violation. *See* Mem. at 15–16.

[10] In *Banknorth v. BJ's Wholesale Club, Inc.*, 394 F. Supp. 2d 283 (D. Me. 2005), the court reserved the issue of duty. The negligence claim was dismissed upon transfer to the Middle District of Pennsylvania. 442 F. Supp. 2d 206, 211–14 (M.D. Pa. 2006) (bank "could have bargained against the risk it incurred, but did not").

Instead, the Banks focus their opposition on a single, auto-delete feature they allege was available for FireEye, but not used by Target. But the Banks admit FireEye was "state of the art" (Compl. ¶ 34), as opposed to "industry standard." A decision not to implement one of its features, therefore, cannot suffice to allege negligence. To hold otherwise would be fundamentally unfair and would discourage investment in security measures. *Funchess*, 632 N.W.2d at 675.

D. <u>The Banks Fail to Allege Negligent Misrepresentation By Omission.</u>

1. *No Duty.*

In the negligent misrepresentation context, a duty arises only where a defendant is engaged in the business or profession of supplying guidance to plaintiffs. *See* Mem. at 17–20.

The Banks concede no such relationship exists here, relying on a supposed "special circumstances" exception to this standard. Opp'n at 39. But the only case they cite in support of this "exception" involved a claim under Minnesota's Consumer Fraud Act, not a claim for negligent misrepresentation. *See Graphic Commc'ns Local 1B Health & Welfare Fund "A" v. CVS Caremark Corp.*, 850 N.W.2d 682, 694–97 (Minn. 2014). It is therefore inapposite.[11] The Banks also cite *M. H. v. Caritas Family Services* to argue Target *assumed* a duty, but nothing in *Caritas* disturbs the rule that a duty arises only in a "professional," "fiduciary," or "advisor" relationship. *Williams v. Smith*, 820

[11] Even if the Banks had alleged a consumer fraud claim, they would have failed to plead duty because they nowhere allege Target made any statements *to them* in the context of a transaction, or that Target's supposed "special knowledge" was knowledge "of fraudulent conduct." *Id.* at 695, 698.

N.W.2d 807, 817–18 (Minn. 2012) (no duty between "sophisticated business people"; *Caritas* involved "special legal relationship").

2. *No Actionable Omission.*

The lone representation the Banks' opposition attributes to Target is a Privacy Policy from Target's website.[12] But the *Complaint* does not identify that Privacy Policy or set forth its contents. Even had the Privacy Policy been attached to the Complaint, the Banks' claim would still not satisfy Rule 9(b), as the Banks do not state if, how, or when they viewed the Privacy Policy, or how it was directed to them for guidance in their transactions. *See Riley v. Cordis Corp.*, 625 F. Supp. 2d 769, 786–87 (D. Minn. 2009). If they had, the Privacy Policy itself would render such allegations implausible, as it clearly is directed only to *consumers*. *See* Opp'n at Rudd Decl., Ex. A (using "you" throughout to refer to Target guests).

Further, the Privacy Policy's alleged omissions are not actionable. The Banks allege that Target "held itself out" as having measures "sufficient to protect" consumers' information (Compl. ¶ 128), but the Privacy Policy contains no such statement, and even explicitly warns consumers about the possibility of intrusions. *See* Privacy Policy at *4 (warning no "system is completely secure or 'hacker proof.'").

The Banks attempt – improperly – to go beyond their allegations to argue that the Privacy Policy deceptively claimed Target used "industry standard methods" to secure

[12] The Banks do not refute that dismissal is appropriate with respect to the purported omissions relating to Target's compliance with Card Operating Regulations or PCI-DSS, and the timing of communications about the Intrusion. *See* Mem. at 22–25. These claims, therefore, should be deemed abandoned, and dismissed. *See, e.g.*, *Gharwal v. Fed. Nat'l Mortg. Ass'n*, No. 13–685, 2013 WL 4838904, at *1 n.2 (D. Minn. Sept. 11, 2013).

payment card data while purportedly omitting that "it did not follow industry protocols" and did not use FireEye's auto-delete feature. Opp'n at 40, 41 n.6. As discussed above, however, the Complaint does not identify any "industry standard method[]" that Target failed to implement and, as for FireEye, a decision not to implement one of its features could have no bearing on whether Target had "industry standard methods" in place. *See supra*, at Part I.C.2.

3. *Reliance Required.*

The only case the Banks cite for the proposition that they are not required to plead reliance on omissions contains no such holding. In fact, like the cases cited in Target's opening brief, *Smith v. Questar Capital Corp.* expressly held that "justifiable reliance" is a required element. No. 12-cv-2669, 2014 WL 2560607, at *13 (D. Minn. June 6, 2014); *see* Mem. at 25–26. Indeed, the *Smith* court relied in part on the alleged omissions to determine that the plaintiff had met its burden to plead reliance, *id.* at *15 – something the Banks have not even attempted here.

II. CONCLUSION

Accordingly, Target respectfully requests that the Court dismiss the Complaint with prejudice.

Respectfully submitted,

Date: October 22, 2014

/s/ Michael A. Ponto

Michael A. Ponto, #203944
Wendy J. Wildung, #117055
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

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.	**LR 7.1(f) and LR 7.1(h) CERTIFICATE OF COMPLIANCE**

I, Michael A. Ponto, certify that Defendant's Reply to Plaintiffs' Opposition to the Motion to Dismiss the Consolidated Class Action Complaint complies with Local Rules 7.1(f).

I further certify that, in preparation of this memorandum, I used 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.

I further certify that the above referenced memorandum contains 3,143 words, exclusive of the caption and signature block.

The cumulative total word count for defendant's memorandum in support filed on September 2, 2014 (8,856 words) and this reply memorandum is 11,999 words.

Date: October 22, 2014

/s/ Michael A. Ponto
Michael A. Ponto, #203944
Wendy J. Wildung, #117055
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