UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation,

MDL No. 14-2522 (PAM/JJK)

This document relates to:
Financial Institution Cases.

MEMORANDUM AND ORDER

This matter is before the Court on Defendant Target Corporation's Motion to Dismiss the Consolidated Amended Class Action Complaint (Docket No. 163) in the Financial Institution Cases. For the reasons that follow, the Motion is granted in part and denied in part.

BACKGROUND

In December 2013, Defendant Target Corporation, a Minnesota-headquartered retailer that is one of the nation's largest retail chains, announced that over a period of more than three weeks during the busy Christmas holiday shopping season, computer hackers had stolen credit- and debit-card information for approximately 110 million of Target's customers. Lawsuits soon followed this announcement, and ultimately the Judicial Panel on Multidistrict Litigation consolidated all federal lawsuits into this litigation. The multidistrict litigation consists of two distinct types of claims: those brought by consumers and those brought by financial institutions. The Motion at issue here seeks to dismiss only the Consolidated Amended Class Action Complaint[1] (Docket No. 163) filed in the financial institution cases.

---

[1] The Court will refer to this pleading as the Complaint.

The court in another consumer data breach case has succinctly described the nation's credit- and debit-card system as follows:

> Every day, merchants swipe millions of customers' payment cards. In the seconds that pass between the swipe and approval (or disapproval), the transaction information goes from the point of sale, to an acquirer bank, across the credit-card network, to the issuer bank, and back. Acquirer banks contract with merchants to process their transactions, while issuer banks provide credit to consumers and issue payment cards. The acquirer bank receives the transaction information from the merchant and forwards it over the network to the issuer bank for approval. If the issuer bank approves the transaction, that bank sends money to cover the transaction to the acquirer bank. The acquirer bank then forwards payment to the merchant.

In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 574 (S.D. Tex. 2011) (footnote omitted), rev'd in part sub nom. Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013). Plaintiffs here are a putative class of issuer banks whose customers' data was stolen in the Target data breach.

Plaintiffs' Complaint consists of four claims against Target. Count One contends that Target was negligent in failing to provide sufficient security to prevent the hackers from accessing customer data. Count Two asserts that Target violated Minnesota's Plastic Security Card Act, and Count Three alleges that this violation constitutes negligence per se. Count Four claims that Target's failure to inform Plaintiffs of its insufficient security constitutes a negligent misrepresentation by omission.

Target now seeks dismissal of all claims, arguing that Plaintiffs have failed to plead sufficient facts to establish any of their claims.

DISCUSSION

When evaluating a motion to dismiss under Rule 12(b)(6), the Court assumes the facts in the Complaint to be true and construes all reasonable inferences from those facts in the light most favorable to Plaintiffs. Morton v. Becker, 793 F.2d 185, 187 (8th Cir. 1986). However, the Court need not accept as true wholly conclusory allegations, Hanten v. Sch. Dist. of Riverview Gardens, 183 F.3d 799, 805 (8th Cir. 1999), or legal conclusions that Plaintiffs draws from the facts pled. Westcott v. City of Omaha, 901 F.2d 1486, 1488 (8th Cir. 1990).

To survive a motion to dismiss, 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, 545 (2007). Although a complaint need not contain "detailed factual allegations," it must contain facts with enough specificity "to raise a right to relief above the speculative level." Id. at 555. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements," will not pass muster under Twombly. Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citing Twombly, 550 U.S. at 555). In sum, this standard "calls for enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of [the claim]." Twombly, 550 U.S. at 556.

A. Negligence

The parties agree that, at least for the purposes of this Motion, Minnesota law governs Plaintiffs' negligence claim. A claim of negligence under Minnesota law requires a plaintiff to allege four elements: duty, breach, causation, and injury. Schmanski v. Church of St.

Casimir of Wells, 67 N.W.2d 644, 646 (Minn. 1954). Target contends that Plaintiffs have failed to sufficiently allege that Target owed them a duty or that Target breached any duty.

1. Duty

Minnesota law imposes a duty "to act with reasonable care for the protection of others" in two situations:

> First, . . . general negligence law imposes a general duty of reasonable care when the defendant's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff. See 1 J.D. Lee & Barry A. Lindahl, Modern Tort Law: Liability & Litigation § 3.48 (2d ed. 2003).
>
> Second, a defendant owes a duty to protect a plaintiff when action by someone other than the defendant creates a foreseeable risk of harm to the plaintiff and the defendant and plaintiff stand in a special relationship. See Bjerke v. Johnson, 742 N.W.2d 660, 665 (Minn. 2007). In other words, although a defendant generally does not have a duty "to warn or protect others from harm caused by a third party's conduct," H.B. ex rel. Clark v. Whittemore, 552 N.W.2d 705, 707 (Minn.1996), an exception to this rule exists when the parties are in a special relationship and the harm to the plaintiff is foreseeable.

Domagala v. Rolland, 805 N.W.2d 14, 23 (Minn. 2011). The existence of a duty is a question of law. ServiceMaster of St. Cloud v. GAB Bus. Servs., Inc., 544 N.W.2d 302, 307 (Minn. 1996).

Target contends that Plaintiffs' claims must be analyzed as falling under the third-party-harm type of negligence, so that to be liable Target and Plaintiffs must stand in a "special relationship" with one another. Target asks the Court to find as a matter of law that Target had no duty to Plaintiffs because there is no special relationship between Plaintiffs and Target and, in any event, "'a person has no duty under Minnesota law to protect another from the harmful conduct, including criminal conduct, of a third person.'" (Def.'s Supp.

Mem. (Docket No. 185) at 6 (quoting RKL Landholding, LLC v. James, No. A12-1739, 2013 WL 2149979, at *2 (Minn. Ct. App. May 20, 2013)).)

Plaintiffs argue that this case is not a third-party-harm case but rather is a straightforward negligence case: Target's own conduct, in failing to maintain appropriate data security measures and in turning off some of the features of its security measures, created a foreseeable risk of the harm that occurred, and Plaintiffs were the foreseeable victims of that harm.

Plaintiffs also argue that, even if this situation is a third-party-harm situation where a special relationship between Plaintiffs and Target is required, they have pled such a special relationship here. But as Target points out, Minnesota has recognized this "separate and distinct" special relationship doctrine, Domagala, 805 N.W.2d at 23, in a very few, limited situations that are not applicable here. See RKL Landholding, 2013 WL 2149979, at *2 (noting that the "'special relationship' exception is a narrow one"). Moreover, the Minnesota Supreme Court has cautioned against extending those situations further. See Whittemore, 552 N.W.2d at 709 (stating that "this court has carefully carved out" the "outer boundaries" of the special relationship exception).

At this preliminary stage of the litigation, Plaintiffs have plausibly pled a general negligence case. Although the third-party hackers' activities caused harm, Target played a key role in allowing the harm to occur. Indeed, Plaintiffs' allegation that Target purposely disabled one of the security features that would have prevented the harm is itself sufficient to plead a direct negligence case: Plaintiffs allege that Target's "own conduct create[d] a

foreseeable risk of injury to a foreseeable plaintiff." Domagala, 805 N.W. 2d at 23. Thus, the Court must determine whether Plaintiffs have sufficiently pled that Target owed Plaintiffs a duty of care under general negligence principles.

Minnesota courts have considered the following factors when determining whether a defendant owed a duty of care in a general negligence case: (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. Domagala, 805 N.W.2d at 26. The duty to exercise reasonable care arises from the probability or foreseeability of injury to the plaintiff. Id. "Although in most cases the question of foreseeability is an issue for the jury, the foreseeability of harm can be decided by the court as a matter of law when the issue is clear." Foss v. Kincaid, 766 N.W.2d 317, 322-23 (Minn. 2009). The Court evaluates Plaintiffs' allegations regarding these factors in the light most favorable to Plaintiffs, keeping in mind that this Motion tests only the sufficiency of those allegations and not the ultimate success of Plaintiffs' legal theories.

Plaintiffs have plausibly alleged that Target's actions and inactions—disabling certain security features and failing to heed the warning signs as the hackers' attack began—caused foreseeable harm to Plaintiffs. Plaintiffs have also plausibly alleged that Target's conduct both caused and exacerbated the harm they suffered. And Plaintiffs' allegation that Target was solely able and solely responsible to safeguard its and Plaintiffs' customers' data is also

plausible. Imposing a duty on Target in this case will aid Minnesota's policy of punishing companies that do not secure consumers' credit- and debit-card information. See Minn. Stat. § 325E.64. And despite Target's dire warnings about the burden of imposing such a duty, it is clear that the institutional parties to credit- and debit-card transactions have already voluntarily assumed similar duties toward one another. See, e.g., In re Heartland, 834 F. Supp. 2d at 588 (noting that Visa and MasterCard Card Operating Regulations, which apply between merchants, issuer banks, and acquirer banks, specify procedures for issuer banks to make claims in the event of data breaches).

That Plaintiffs have plausibly alleged a duty on Target's part is bolstered by the existence of Minnesota's Plastic Card Security Act, discussed in more detail below. While courts are reluctant to recognize duties of care in the absence of legislative imprimatur, the duty to safeguard credit- and debit-card data in Minnesota has received that legislative endorsement. And the legislature specifically acknowledged the availability of other causes of action arising out of a Minnesota company's failure to safeguard customers' information, stating that the remedies under the PCSA "are cumulative and do not restrict any other right or remedy otherwise available" to the issuer banks. Minn. Stat. § 325E.64, subd. 3. Plaintiffs have adequately pled that Target owed them a duty of care, and their negligence claim will not be dismissed on this basis.

2. Breach

Having determined that Plaintiffs have plausibly alleged the existence of a duty, there can be no doubt that Plaintiffs have also plausibly alleged that Target breached that duty by

failing to safeguard Plaintiffs' customers' information. Because Target does not challenge Plaintiffs' allegations with respect to the elements of causation and damages, Plaintiffs' negligence claim succeeds in stating a claim on which relief can be granted.

B. Negligent Omission

Plaintiffs' negligent-misrepresentation-by-omission claim alleges that Target "failed to disclose material weaknesses in its data security systems and procedures" that it had an obligation to disclose. (Compl. ¶ 131.) According to Target, this claim fails for multiple reasons: Target had no duty to disclose anything to Plaintiffs; Plaintiffs have failed to plead this claim with the particularity Rule 9(b) requires; a negligent misrepresentation claim does not lie with respect to statements about Target's intent; and Plaintiffs have failed to allege reliance, which is an essential element of a negligent-misrepresentation-by-omission claim.

1. Duty

"As a general rule, one party to a transaction has no duty to disclose material facts to the other." Smith v. Questar Capital Corp., Civ. No. 12-2669, 2014 WL 2560607, at *14 (D. Minn. June 6, 2014) (Nelson, J.). This rule applies "unless (1) there existed a fiduciary or confidential relationship between the parties; (2) one party was in possession of special facts that could not have been discovered by the other; or (3) one party who chooses to speak omits information so as to make the information actually disclosed misleading." Id. (citing Sailors v. N. States Power Co., No. 4:02-253, 1992 WL 532172, at *9 (D. Minn. July 13, 1992) (MacLaughlin, J.); Klein v. First Edina Nat'l Bank, 196 N.W.2d 619, 622 (Minn. 1972)).

Plaintiffs have not alleged that there is a fiduciary or confidential relationship between Target and Plaintiffs. Rather, Plaintiffs contend that Target knew facts about its ability to repel hackers that Plaintiffs could not have known, and that Target's public representations regarding its data security practices were misleading. Target takes issue with Plaintiffs' allegations in this regard, but on a Motion to Dismiss, the Court must determine only whether the allegations are plausible. The allegations meet that plausibility standard, and Plaintiffs have adequately pled a duty of care.

2. Rule 9(b)

Target also argues that Plaintiffs' negligent omission claim should be dismissed for failure to comply with the stricter pleading requirements of Rule 9(b). The Rule requires that, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). These heightened pleading requirements apply to negligent-misrepresentation-by-omission claims. Trooien v. Mansour, 608 F.3d 1020, 1028 (8th Cir. 2010). In the context of a claim of negligent omission, the Rule is satisfied "if the omitted information is identified and 'how or when' the concealment occurred." In re Bisphenol-A (BPA) Polycarbonate Plastic Prods. Liab. Litig., 687 F. Supp. 2d 897, 907 (W.D. Mo. 2009) (citing Great Plains Trust Co. v. Union Pac. R. Co., 492 F.3d 986, 996 (8th Cir. 2007)).

Plaintiffs have identified the omitted information, namely Target's failure to disclose that its data security systems were deficient and in particular that Target had purposely disengaged one feature of those systems that would have detected and potentially stopped

the hackers at the inception of the hacking scheme. Plaintiffs contend that these omissions were made in representations such as Target's online Privacy Policy and in Target's agreement to comply with Visa and MasterCard's Card Operating Regulations and other security requirements.

Although these allegations are not as detailed as Target would like, at this early stage of the litigation they are sufficient to allege the "how or when" the information regarding Target's data security practices was omitted from disclosure. Plaintiffs have complied with 9(b).

3. Omissions

Target argues that Plaintiffs' claim is not cognizable because it is founded on alleged omissions regarding what Target intended to do with respect to data security. Target contends that an omission regarding Target's "present intention to act in the future" is not actionable because it cannot be proved false. (Def.'s Supp. Mem. (Docket No. 185) at 23.) But Target misconstrues Plaintiffs' claim. Plaintiffs' negligent-omission claim is not premised on any statement about Target's future intentions or even on Target's statements about the data breach itself, but rather on the fact that Target held itself out as having secure data systems when Target knew that it did not have secure systems and had taken affirmative steps to make its systems more vulnerable to attack. At this stage of the case, this allegation is sufficient to state a claim for negligent omission.

4. Reliance

Finally, Target contends that Plaintiffs have failed to plead any reliance on the alleged omissions. Plaintiffs respond that reliance is not required, citing Judge Nelson's recent Smith decision. (Pls.' Opp'n Mem. (Docket No. 204) at 41.) But Smith did not hold that reliance is not a required element for a negligent omission claim. Rather, Smith found that reliance was a "fact-intensive" inquiry inappropriate for resolution on a motion to dismiss. Smith, 2014 WL 2560607, at *15.

A plaintiff raising a securities fraud-by-omission claim need not plead or prove reliance if the omitted information is material—reliance on that material information is presumed. Affiliated Ute Citizens v. United States, 406 U.S. 128, 153-54 (1972). But courts have not extended this presumption of reliance outside of the securities-fraud context. Plaintiffs are therefore required to plead reliance on Target's alleged omissions in order to state a claim for relief.

The Complaint contains no indication that Plaintiffs relied on any of the alleged omissions. Rather, the Complaint merely avers that Plaintiffs "suffered injury" "as a direct and proximate result of Target's negligent misrepresentations by omission." (Compl. ¶ 134.) This is insufficient to plead reliance, and Plaintiffs' negligent-misrepresentation-by-omission claim must therefore be dismissed. Assuming that there are facts supporting Plaintiffs' reliance on the alleged omissions, Plaintiffs may file an amended complaint within 30 days that fully and plausibly alleges all of the required elements of a negligent-misrepresentation-by-omission claim.

C. Plastic Card Security Act

Minnesota's Plastic Card Security Act provides:

> No person or entity conducting business in Minnesota that accepts a[] [credit or debit card] in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.
>
> * * * *
>
> Whenever there is a breach of the security of the system of a person or entity that has violated this section . . . that person or entity shall reimburse the financial institution that issued any [credit or debit cards] affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders . . . .

Minn. Stat. § 325E.64, subd. 2, 3. Count Two of the Complaint alleges a violation of this section, and Count Three contends that as a result of the alleged violation of the PCSA, Target is negligent per se.

Target raises two challenges to Plaintiffs' PCSA claims. First, Target contends that the PCSA applies only to transactions that occur in Minnesota, making the Act inapplicable to the majority of transactions about which Plaintiffs complain. Second, Target argues that the PCSA only prohibits the retention of customer data, and because the customer data at issue here was stolen when the consumer's card was used at a Target store and was not stolen from Target's database, Target's alleged retention of that data did not cause Plaintiffs' claimed harm.

Target's first argument is not well taken. The Act does not apply only to business transactions that take place in Minnesota. By its terms, it applies to the data retention practices of any person or entity "conducting business in Minnesota." Minn. Stat. § 325E.64, subd. 2. Target is a Minnesota company that conducts business in Minnesota, and thus its data retention practices are governed by the Act. And contrary to Target's assertions, the application of the PCSA to out-of-state transactions does not implicate the dormant Commerce Clause. See Jones v. Gale, 470 F.3d 1261, 1267 (8th Cir. 2006) (state law violates dormant Commerce Clause if it legislates "'differential treatment of in-state and out-of-state economic interests that benefits the former and burdens the latter'") (quoting, among others, Oregon Waste Sys., Inc. v. Dep't of Envtl. Quality, 511 U.S. 93, 99 (1994)). The PCSA does not discriminate between in-state and out-of-state transactions or economic interests. Rather, it applies only to Minnesota companies' data security practices and does not purport to regulate the practices of any non-Minnesota company. And it applies equally to the Minnesota companies' data retention practices with respect to in-state and out-of-state transactions. The dormant Commerce Clause does not render the application of the PCSA in this situation unconstitutional.

Target's second argument is that, even if Target violated the retention provisions of the Act as Plaintiffs allege, Target's allegedly illegal activities did not cause the harm of which Plaintiffs complain. There is no dispute that the hackers who stole Target's customers' data did so by installing malware on Target's computer servers that read the data from customers' credit and debit cards at the moment those cards were swiped in Target's stores. Thus,

according to Target, the fact that Target may also have stored that data longer than the PCSA allows is irrelevant, because the hackers did not steal the data from Target's data storage but rather stole it directly from the cards as they were used in Target's stores. Plaintiffs' response to this argument is two-fold. First, they allege that the hackers' malware did not immediately transmit the stolen data to the hackers' servers, but rather stored the stolen data on Target's own servers for up to six days before transmitting that data to the hackers. Thus, Plaintiffs contend that Target's servers did "retain" the data within the meaning of the PCSA, and that retention allowed the hackers to steal that data. Plaintiffs also contend that the hackers would have been unable to steal all of the magnetic stripe information, in particular the card's CVV code, without accessing the customer data Target regularly stored on its servers. In other words, Plaintiffs assert that the hackers gathered some data from the use of the card and other data from Target's servers, making the data breach even more serious.

Plaintiffs and Target disagree over which definition of "retain" the Court should use in interpreting the PCSA's requirements. Plaintiffs urge the Court to adopt the Oxford Dictionary's definition of retain, which is to "continue to have something." (Pls.' Opp'n Mem. at 12.) Target, on the other hand, contends that the correct definition of "retain" must be read in the context of technical data retention, and is "the storage of data for future usage." (Def.'s Reply Mem. (Docket No. 221) at 2 (emphases omitted)).[2]

[2] Perhaps realizing that this definition does not sufficiently help its argument, Target takes it a step further and contends that the PCSA applies only if the entity "affirmatively stores [data] for its own future use." (Id.) Thus, according to Target, even if the hackers stored the stolen data on Target's servers, Target did not "retain" that data within the PCSA's

Whether the Court interprets "retain" to mean "to continue to have" or "storage for future use" is immaterial to the outcome of the Motion to Dismiss. Plaintiffs allege that Target stored data for longer than the PCSA allows, and that the hackers were able to access some of this stored data, namely the CVV codes, without which the breach would not have been as serious. In other words, although the hackers received some data directly from consumers' cards, they also retrieved other data from Target's servers. Even if Target is correct that the hackers' storage of stolen data on Target's servers does not implicate the PCSA, Plaintiffs' claims undoubtedly state a PCSA violation. The Motion to Dismiss this Count must be denied.

Because Target's only argument regarding the negligence per se claim is that it fails because the PCSA claim fails, the negligence per se claim likewise survives this Motion.

CONCLUSION

Plaintiffs have plausibly pled a claim for negligence, a violation of the PCSA, and negligence per se. Plaintiffs failed to plead reliance, however, and therefore their negligent-misrepresentation claim must be dismissed without prejudice.

Accordingly, **IT IS HEREBY ORDERED that**:

1. Defendant's Motion to Dismiss the Financial Institution Cases (Docket No. 183) is **GRANTED in part** and **DENIED in part**;

---

definition. Target's insistence that "retain" applies only to data the entity stores for its own use, however, is not supported by the authorities Target cites.

2. The negligent-misrepresentation claim (Count Four) is **DISMISSED without prejudice**; and

3. Plaintiffs shall have 30 days from the date of this Order to file an Amended Complaint sufficiently alleging the required elements of their negligent-misrepresentation claim, should they wish to do so.

Dated: December 2, 2014

s/ Paul A. Magnuson
Paul A. Magnuson
United States District Court Judge