New York Law Journal | dbr DAILY BUSINESS REVIEW

A NEW YORK LAW JOURNAL SPECIAL SECTION

An ALM Publication

WWW.NYLJ.COM

MONDAY, JUNE 6, 2016

Cybersecurity

Defending A Data Breach Class Action

BY SETH D. ROTHMAN AND DENNIS S. KLEIN

By **Seth D. Rothman**

And **Dennis S. Klein**

Over the past few years, a number of large and highly-publicized data breaches have generated a wave of class action litigation that shows no signs of relenting. Household names, such as eBay, Home Depot, Neiman Marcus, Sony, and Target, have found themselves defending such actions in federal courts throughout the country. Most of these cases have been resolved at the pleading stage through motions to dismiss or strategically-structured settlements. This article discusses the principal defenses that have been raised on motions to dismiss and some ways that data breach settlements have been structured.

Lack of Standing

The primary defense in data breach actions is that plaintiffs lack Article III standing because they have not suffered an "injury-in-fact." To establish Article III standing, the plaintiffs' injuries must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[1] Data breach plaintiffs are typically able to allege that their personal information has been stolen, but this may not be enough to establish standing if the theft has not led to any out-of-pocket loss.

Courts have dismissed data breach cases for lack of standing where plaintiff could not plead that his stolen information "was misused or that his identity was stolen as a result of the data theft,"[2] where plaintiffs alleged only that criminals "may" hold their personal information,[3] where plaintiffs alleged that defendant's delay in notifying them of the data breach "increased the risk to Plaintiffs of suffering some actual injury due to the security breach,"[4] where plaintiffs failed to allege "to have detected any irregularity whatsoever in regards to unauthorized purchases or other manifestations that their personal information has been misused,"[5] and where plaintiff alleged only that there had been an attempt to use her stolen credit card information.[6]

In assessing whether there has been an out-of-pocket loss, courts look to whether plaintiffs have had to bear the cost of fraudulent charges or identity theft. If those costs have been reimbursed by a credit card company or a financial institution, plaintiffs may not be able to satisfy

SETH D. ROTHMAN *and* DENNIS S. KLEIN *are litigation partners at Hughes Hubbard & Reed. Associates* TYLER GROVE *and* JEFFREY GOLDBERG *contributed to the preparation of this article.*

this requirement. Courts have also been unwilling to recognize mitigation efforts as cognizable injuries. The time and effort that plaintiffs spend to protect themselves from the data breach may not suffice to confer standing.[7]

Other courts, including the U.S. Court of Appeals for the Seventh Circuit, have been willing to find standing in the absence of economic injury. In the *Neiman Marcus* and *P.F. Chang's* data breach litigations, the Seventh Circuit found that the theft of credit card information was a concrete enough injury to confer standing "because a primary incentive for hackers is 'sooner or later to make fraudulent charges or assume those customers' identities.'"[8] The Seventh Circuit also held that "the time and money resolving fraudulent charges are cognizable injuries for Article III standing."[9]

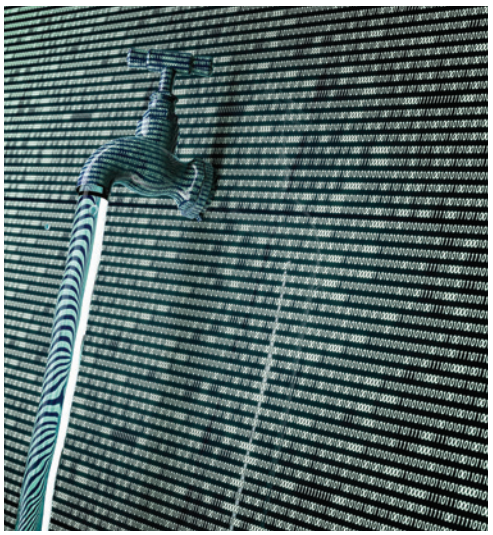
The courts that have allowed data breach claims to proceed have generally emphasized that their holdings are limited to the pleadings stage. These courts are not commenting on class certification issues or the merits of the case. Indeed, the court in the *Target* litigation specifically cautioned that "should discovery fail to bear out Plaintiffs' allegations, Target may move for summary judgment on the issue."[10]

In an effort to avoid the problems of pleading standing, some data breach plaintiffs have asserted statutory causes of action. Courts have generally been reluctant to find statutory standing in the absence of a concrete injury.[11] This issue was recently addressed by the U.S. Supreme Court in *Spokeo v. Robins*,[12] where the court confirmed that Article III standing requires a concrete injury even in the context of a statutory violation.

Plaintiffs must show a **temporal and logical connection** between the data breach and their alleged injuries. Courts have dismissed claims where the plaintiffs have failed to plead or later prove facts that connect the data breach to their injuries.

Insufficient Causation

Data breach defendants have also asserted that plaintiffs have failed to plead an adequate connection between the alleged data breach and their alleged loss. This usually arises both as part of the standing analysis—since plaintiffs must show that their injuries are fairly traceable to the data breach—and in connection with plaintiffs' substantive causes of action. Plaintiffs typically plead negligence as their primary cause of action and must therefore allege direct and proximate causation.



The "fairly traceable" requirement for standing requires a lesser showing than direct and proximate cause,[13] but, in practice this may be a distinction without a difference. Either way, plaintiffs must show a temporal and logical connection between the data breach and their alleged injuries.[14] Courts have dismissed claims where the plaintiffs have failed to plead or later prove facts that connect the data breach to their injuries.[15]

Defendants may also be able to show that the negligence of a third-party vendor was an intervening and superseding cause of the data breach. Hackers will sometimes use a vendor's credentials to access companies' sensitive information, and this gives rise to an argument that the vendor's negligence caused the breach.[16] One breached company has even gone so far as to sue its IT vendor for negligence.[17]

Strategic Settlement Structures

The high-profile settlements in the *Target* ($10 million) and *Home Depot* ($19.5 million) cases have drawn attention to the ways in which data breach settlements may be quantified and structured. The *Target* and *Home Depot* settlements were relatively high for data breach cases, but both of these cases involved large numbers of potential plaintiffs. The data breach at Target was estimated to have affected approximately 110 million customers. Prior to settling, Target reviewed recent data breach settlements and found that these cases settled on average for less than 50 cents per person.[18]

Unlike settlements in traditional cases, data breach settlements do not necessarily attempt to compensate plaintiffs for out-of-pocket loss. Indeed, many plaintiffs do not have out-of-pocket losses because their credit card companies and financial institutions have reimbursed them.[19] The Home Depot settlement consisted of $13 million to compensate plaintiffs for the time and effort they spent resolving issues arising from the theft of their personal information and $6.5 million to fund 18 months of credit monitoring.[20]

Conclusion

Data breaches continue to occur with alarming frequency. While not every data breach leads to litigation, the large, high-profile data breaches usually do. Targeted companies have been relatively successful at resolving these cases through motions to dismiss and settlements. But the stakes are getting higher, and plaintiffs' lawyers will continue to refine their pleadings to address some of the problems they have faced in the past. Companies need to be prepared to defend themselves aggressively.

1. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1140 (2013) (quoting *Monsanto v. Geertson Seed Farms*, 130 S. Ct. 2743 (2010)).

2. *Galaria v. Nationwide Mut. Ins.*, 998 F. Supp. 2d 646, 650, 654-60 (S.D. Ohio 2014).

3. *Green v. eBay*, No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015).

4. *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013).

5. See Order, *In re Zappos.com, Customer Data Sec. Breach Litig.*, No. 3:12-cv-00325-RCJ-VPC, MDL No. 2357, at *12 (D. Nev. June 1, 2015) (ECF No. 235); see also id. at *7-9 (listing cases holding that "absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing").

6. See Memorandum & Order, *Whalen v. Michael Stores*, No. 2:14-cv-07006-JS-ARL, at 6-9 (E.D.N.Y. Dec. 28, 2015) (ECF No. 29) (Whalen Order).

7. See, e.g., *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588 at *4-5.

8. Final Opinion of the Court, *Lewert v. P.F. Chang's China Bistro*, No. 14-3700, at 6-7 (7th Cir. April 14, 2016) (ECF No. 38) (citing *Remijas v. Nieman Marcus Grp.*, 794 F.3d 688 (7th Cir. 2015)).

9. Id. at 7. See also Minute Order, *Corona v. Sony Pictures Entm't*, No. 14-cv-09600 RGK (Ex), at 3 (C.D. Cal. June 15, 2015) (ECF No. 97); *In re Target Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014).

10. *In re Target Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1159.

11. *Whalen* Order, supra note 6, at 11-12 (discussing N.Y. Gen. Bus. Law §349).

12. 578 U.S. ____ (2016).

13. See *Resnick v. AvMed*, 693 F.3d 1317, 1324 (11th Cir. 2012).

14. See, e.g., id. at 1326-27.

15. See, e.g., *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 31-32 (D.D.C. 2014) (dismissing claim where plaintiffs failed to plead that their banking information was part of the stolen data that supposedly led to fraudulent transactions); *In re Horizon Healthcare Servs. Data Breach Litig.*, No. 13-7418 CCC, 2015 WL 1472483, at *8 (D.N.J. March 31, 2015) (dismissing claim where plaintiff-husband alleged that only his personal information was disclosed); Opinion and Order, *Jones v. Commerce Bank, N.A.*, No. 1:06-cv-00835-HB-FM (S.D.N.Y. March 6, 2007) (ECF No. 51) (granting defendant's motion for summary judgment due to a lack of evidence of causation).

16. See Shelly Banjo, "Home Depot Hackers Exposed 53 Million Email Addresses," Wall Street Journal, Nov. 6, 2014.

17. Complaint, *Affinity Gaming v. Trustwave Holdings*, No. 2:15-cv-02464-GMN-PAL (D. Nev. Dec. 24, 2015) (ECF No. 1).

18. Exhibit 2, Dec. of Vincent J. Esades, *In re Target Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM) (D. Minn. March 18, 2015) (ECF No. 358-2).

19. The financial institutions have also brought claims against the defendant corporations. As the financial institution bears the actual loss, the settlement with the financial institution may exceed the settlement with the consumer class action plaintiffs. Target's settlement with its consumers' banks ($39.4 million) was nearly four times as large as Target's settlement with its customers ($10 million). Compare Exhibit A (Settlement Agreement and Release), Dec. of Charles Zimmerman, *In re Target Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM) (D. Minn. Dec. 2, 2015) (ECF No. 653-1) with Order, *In re Target Consumer Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM) (D. Minn. March 19, 2015) (ECF No. 364).

20. See Exhibit 1 (Settlement Agreement), Motion for Order Consumer Plaintiffs' Motion for Preliminary Approval of Class Settlement, *In re The Home Depot Customer Data Sec. Litig.*, MDL No. 1:14-md-02583-TWT (N.D. Ga. March 7, 2016) (ECF No. 181-2).