Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lessons From The Target Data Breach Settlement

Law360, New York (May 04, 2015, 10:29 AM ET) --

Stephen Rossi

Law360 recently reported that "29 percent of corporate counsel said they anticipate data privacy will be the next wave of class action litigation."[1] Based on the number of lawsuits stemming from major data breaches suffered by Target Corp., Home Depot Inc., and most recently Anthem Inc., that could be true. But plaintiffs that bring class actions on behalf of consumers affected by a data breach must overcome several legal and practical problems before ever getting their class certified. This results in settlements that frequently set aside just pennies per affected individual in cash compensation — even if the settlement includes large attorneys' fees and other noncash value.

For example, in the case of Target's data breach, at least 40 million customers' credit and debit card numbers were stolen, and the personal information of as many as 110 million people was compromised. The plaintiffs agreed to settle for $10 million in available cash compensation in addition to other (admittedly valuable) noncash benefits like an agreement by Target to implement stricter data security procedures. Although $10 million is nothing to sneeze at, it equates to less than 10 cents per victim in cash compensation. To show that its proposal compared favorably to historical settlements, the Target plaintiffs provided a chart of 11 past data breach settlements. It showed that in cases involving more than 1 million victims, the defendant settled on average for less than 50 cents per person in available cash compensation.[2]

What's going on? One simple answer is that many data breaches cause few compensable injuries to the people whose data is accessed. Credit card holders are usually not responsible for fraudulent charges. Credit and identity theft monitoring can help prevent or mitigate identity theft. And it is hard to prove that any particular person's identity was stolen as a result of a particular breach — let alone doing so on a classwide basis. In contrast, the companies that issue payment cards may have an easier time proving actual damages if they can prove causation. For example, the cost to replace a credit card has been reported to range from $2.99 to $12.75,[3] and card issuers frequently seek reimbursement for those costs from the company that suffered the breach. Target recently settled with MasterCard for $19 million.[4]

The lack of injury to consumers was clearly demonstrated in the Heartland Payment case.[5] There,

hackers stole payment card information for 100 million consumers from a payment processing company. In the settlement, Heartland made up to $2.4 million available to consumers. As in the Target settlement and many other data breach settlements, consumers had to submit information substantiating their injuries in order to claim any of the money. Heartland spent $1.5 million on a campaign meant to ensure that 80 percent of the 100 million member class was notified that they could file a claim for their losses.[6] Only 11 valid claims were made, worth a total of $1,925.[7]

When all was said and done, Heartland spent $270,000 on claims administration costs to pay out less than $2,000.[8] This helps explain why most settlements, including the Target settlement, place significant value on non-cash components such as the defendant's promise to institute operational changes to reduce the risk of future data breaches.

Another simple explanation for low per person cash settlements may be that data breach cases are largely motivated by attorneys' fees. In the Target case, Target set aside $10 million for the consumers and agreed to pay up to $6.75 million in attorneys' fees. In the settlements cited by the Target plaintiffs, the available fees ranged from $200,000 in a case in which the plaintiffs could recover $225,000, to a high of $6.5 million when $10 million was available to the class. Well-compensated plaintiffs' counsel may lack the necessary motivation to fight for higher settlements when they can quickly secure large fee awards.

Finally, two major legal stumbling blocks can also drive down settlement values in consumer data breach class actions. The first is that many plaintiffs lack standing to sue because they fail to plead a legally recognized injury. Second, classes may never be certified because it can be difficult for plaintiffs to show that classwide issues predominate over individual causation and damages issues. Indeed, the Target plaintiffs stated the risks associated with their case "included obtaining and maintaining class certification through trial, … establishing causation, and proving Class Members' damages."[9]

Lack of Standing Is A High Hurdle But Will Not Trip Up All Claims

Recently, many thought that Clapper v. Amnesty International would doom data breach class actions because it seemingly prohibits claims based on the increased risk of identity theft, which is frequently claimed by plaintiffs that cannot show any other injury from a breach. In Clapper, the U.S. Supreme Court addressed the standing requirement that every claimant must satisfy, which includes showing an injury-in-fact. There, the plaintiffs sought to challenge the constitutionality of the Foreign Intelligence Surveillance Act. The plaintiffs' jobs required them to communicate with individuals potentially targeted under the act. They tried to establish injury-in-fact by claiming (1) that there was an objectively reasonable likelihood that their communications would be targeted for surveillance and (2) that they took costly measures to protect the confidentiality of their international sources. Their arguments were rejected.

Clapper first held that only actual or certainly impending injuries satisfied the injury-in-fact requirement.[10] The plaintiffs' claim that they could be subject to surveillance failed to show that the threatened injury was "certainly impending."[11] Second, the court held that standing could not be based on resources spent out of fear of surveillance, because it did not want to allow plaintiffs to "manufacture" standing.

Clapper's effect on data breach cases was significant. Many cases have followed Clapper and found that increased risk of identity theft or other harm is too speculative to satisfy the injury-in-fact requirement.[12] Several have also rejected attempts to manufacture standing based on the costs of

protecting against those future harms.[13]

Unfortunately for defendants, a number of cases, particularly those in California federal court, have continued to follow pre-Clapper precedent holding that increased risk of identity theft is enough to satisfy the injury-in-fact requirement.[14] Those cases have also generally distinguished Clapper on the grounds that the Clapper plaintiffs never alleged that their communications were specifically targeted or approved for surveillance, whereas hackers that deliberately steal information are very likely to misuse the stolen information.[15]

Moreover, some statutes explicitly provide that the disclosure of a person's protected information is an injury per se. For example, a recent case in California federal court denied a motion to dismiss a claim under California's Confidentiality of Medical Information Act because the act makes nominal damages of $1,000 available whether or not the "plaintiff suffered or was threatened with actual damages."[16]

And of course, some courts will find that the plaintiffs alleged actual injury. For example, in a case against LinkedIn, plaintiffs survived a motion to dismiss by pleading they purchased LinkedIn's premium service based on LinkedIn's allegedly false statements regarding the efficacy of its data security procedures. Those allegations were enough to support a claim of economic injury.[17]

In the Target class action, Target made the argument, which is now typical in cases involving payment card information, that only unreimbursed credit card charges or closed accounts qualified as actual injuries. The district court held Target's position "set a too-high standard ... at the motion-to-dismiss stage" and that allegations including "unlawful charges, restricted or blocked access to bank account, inability to pay other bills, and late payment charges or new card fees" were sufficient to satisfy the standing requirement.[18]

Instead of continuing to fight after the motion to dismiss was denied, Target quickly settled. But the plaintiffs recognized that in that case, as in many others, it would be difficult to "obtain[] and maintain[] class certification through trial" and it would be difficult to establish causation and damages.[19]

Individual Causation and Damages Issues May Predominate Over Class Issues

If they survive a motion to dismiss, plaintiffs must get their class certified and maintain certification throughout the case. One issue that has yet to be fully addressed in the data breach context is the predominance requirement as applied to damages and causation. To certify and maintain one common type of class action, the court must find that "the questions of law or fact common to class actions predominate over any questions affecting only individual members."[20]

The Supreme Court gave extra ammunition to defendants seeking to block class certification in Comcast Corp. v. Behrend. It made class certification more difficult by reiterating that plaintiffs must offer a damages theory that "establish[es] that damages are capable of measurement on a classwide basis."[21] District courts must conduct a "rigorous analysis" to ensure certification is proper.[22]

In Comcast, cable television subscribers accused Comcast of antitrust violations. They originally argued four theories of antitrust and their damages model included all four theories. The district court certified only one antitrust theory, but the plaintiffs did not change their damages model. The Supreme Court held that certification of the class on the remaining theory was improper under Rule 23(b)(3) because the damages theory (which still included the three discarded antitrust theories) fell "far short of establishing that damages are capable of measurement on a classwide basis."[23]

After Comcast, many thought that it would be difficult for data breach plaintiffs to satisfy the predominance requirement because damages resulting from the breach — such as identity theft or credit card fraud — can often be very individualized. But following Comcast, some circuits have said that Comcast stood only for the proposition that damages theories must be tied to liability theories, and individualized damages calculations do not automatically defeat Rule 23(b)(3) certification.[24] Thus, the value of Comcast to data breach defendants is in question.

Even before Comcast, however, one district court denied class certification in a data breach case for failure to satisfy the predominance factor. That case may be instructive to future defendants. In In re Hannaford Bros. Co. Customer Data Security Breach Litigation, the district court distinguished between individualized damages issues (which would not defeat class certification) and individualized damages causation issues (which would).[25]

In Hannaford, a grocery store's customers' credit card data was breached. Following a dismissal of earlier claims for lack of standing, the plaintiffs eventually sought to certify a class of people that spent money mitigating the breach by paying fees to replace their credit cards and purchasing credit and identity theft monitoring.[26]

The court found that individual issues will predominate when it came to what caused the alleged damages. It recognized that customers may have replaced their cards or purchased insurance for reasons unrelated to the breach.[27] It also acknowledged that credit card fraud is pervasive and it may have happened for reasons unrelated to the breach. The court denied certification because the plaintiffs had not presented an expert opinion to overcome the predominance issues related to causation and damages.[28]

Taken together with Comcast, Hannaford's analysis may drive down settlement values because plaintiffs may need to present expert opinion to support their novel causation and damages theories before a class can be certified. Few cases have made it that far, so class certification will be an important stage in future data breach cases.

Conclusion

The practical problem with consumer data breach class action cases is that most consumers do not suffer large injuries when a data breach occurs. That causes several legal problems for consumer data breach plaintiffs. Although Clapper did not eliminate consumer data breach class actions, plaintiffs will frequently have to claim an injury worse than an increased risk of future harm. Similarly, Comcast may not prevent certification of all data breach classes, but it reinforces the district court's obligation to strictly scrutinize motions for class certification. It also potentially raises the bar for plaintiffs by forcing them to provide early expert opinions that satisfy the predominance requirement. These issues all combine to encourage lower settlements.[29]

—By Stephen Rossi, Irell & Manella LLP

Stephen Rossi is an associate in Irell & Manella's Newport Beach, California, office.

[1] Melissa Maleske, GC Facing More Class Actions, Higher-Exposure Cases, Law360, March 17, 2015, available at http://www.law360.com/california/articles/632403?nl_pk=c6396d23-d942-4088-b08d-191a99c29a40&utm_source=newsletter&utm_medium=email&utm_campaign=california (Citing survey by Carlton Fields Jorden Burt LLP).

[2] In re Target Corp. Customer Data Sec. Breach Litig., No. MDL 14-2522 PAM/JJK, Dkt. No. 358-2 (D. Minn. March 16, 2015). The amounts set aside for classes under 1 million tended to be several times higher per person.

[3] Penny Crosman, How Much Do Data Breach Costs? Two Studies Attempt a Tally, American Banker (September 11, 2014) available at http://www.americanbanker.com/issues/179_176/how-much-do-data-breaches-cost-two-studies-attempt-a-tally-1069893-1.html.

[4] Allison Grande, Target Strikes $19M Deal with MasterCard Over Data Breach, Law360 (April 15, 2015) available at http://www.law360.com/banking/articles/643901.

[5] See In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040 (S.D. Tex. 2012).

[6] Id. at 1077-78.

[7] Id. at 1075.

[8] Id. at 1078.

[9] In re Target Corp. Data Sec. Breach Litig., No. MDL 14-2522 PAM/JJK, Dkt. No. 357 at 28 (D. Minn. March 18, 2015).

[10] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

[11] Id. at 1147.

[12] Storm v. Paytime, Inc., No. 14-CV-1138, 2015 WL 1119724, at *6 (M.D. Pa. Mar. 13, 2015) ("[T]he Court finds no factual allegation of misuse or that such misuse is certainly impending … [and] we find that Plaintiffs have not alleged an actual injury."); Peters v. St. Joseph Servs. Corp., No. 4:14-CV-2872, 2015 WL 589561, at *5 (S.D. Tex. Feb. 11, 2015) ("Peters' alleged future injuries are speculative-even hypothetical-but certainly not imminent. Critically, Peters 'cannot describe how [she] will be injured without beginning the explanation with the word if.'"); Lewert v. P.F. Chang's China Bistro, Inc., No. 14-CV-4787, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014) ("Plaintiffs do not allege that identity theft has occurred; rather, they allege that identity theft may happen in the coming years. Plaintiffs have not alleged an injury in fact with respect to identity theft."); Tierney v. Advocate Health & Hospitals Corp., No. 13 CV 6237, 2014 WL 5783333, at *2 (N.D. Ill. Sept. 4, 2014) (accord); Strautins v. Trustwave Holdings, Inc., No. 12-C-09115, 2014 WL 960816, at *4 (N.D. Ill. Mar. 12, 2014) ("Clapper compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing."); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 655 (S.D. Ohio 2014) (accord); In re Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) ("Merely alleging an increased risk of identity theft or fraud is insufficient to establish standing."); Hammer v. Sam's E., Inc., No. 12-CV-2618-CM, 2013 WL 3756573, at *3 (D. Kan. July 16,

2013) (accord). See also Remijas v.Neiman Marcus Grp., LLC, No. 14 C 1735, 2014 WL 4627893, at *3 (N.D. Ill. Sept. 16, 2014) (holding that only unreimbursed credit card charges would satisfy standing requirement and that there was no certainly impending risk of identity theft).

[13] E.g., Peters v. St. Joseph Servs. Corp., No. 4:14-CV-2872, 2015 WL 589561, at *5 (S.D. Tex. Feb. 11, 2015) ("Peters would therefore still fall short of the constitutional standard if she asserted any money spent prophylactically on credit monitoring services to 'ease fears of future third-party criminality.'"); Polanco v.Omnicell, Inc., 988 F. Supp. 2d 451, 470 (D.N.J. 2013) (accord).

[14] See, e.g., In re Adobe Sys., Inc. Privacy Litig., No. 13-CV-05226-LHK, 2014 WL 4379916, at *6-8 (N.D. Cal. Sept. 4, 2014) (distinguishing Clapper and continuing to follow Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010)); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961-62 (S.D. Cal. 2014) (accord and finding wrongful disclosure of information sufficient to confer standing); Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014) (following Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) and stating "I respectfully disagree with my colleagues that Clapper should be read to overrule Pisciotta's holding that an elevated risk of identity theft is a cognizable injury-in-fact."). See also Reilly v. Ceridian Corp., 664 F.3d 38, 43-44 (3d Cir. 2011) (identifying Circuit split and holding that the threat of future identity theft was insufficient to confer standing).

[15] In re Adobe, 2014 WL 4379916 at 8-9. On the other-hand, when there is no indication that misuse of data will likely occur, some of those cases still recognize that the plaintiffs may lack standing. For example, when a laptop is stolen and there is no allegation that (1) it was stolen for the purpose of misappropriating information for identity theft purposes or (2) such misuse has occurred, the claimed injury may still be too "highly attenuated" to satisfy Clapper. Id. at 9; In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. MDL 2360, 2014 WL 1858458, at *6-9 (D.D.C. May 9, 2014) (explaining that the theft of data tapes was insufficient to grant standing without specific allegations of misuse because "the alleged future injury depends on the actions of an independent third party" that may not even know what it has). See also Storm v. Paytime, Inc., No. 14-CV-1138, 2015 WL 1119724, at *7 (M.D. Pa. Mar. 13, 2015) ("Based on the failure to allege facts showing a misuse of data or that such misuse is imminent, Clapper and Reilly direct us to dismiss Plaintiffs for lack of standing without too much hesitation. This disposition is in line with the vast majority of courts who have reviewed data breach cases where no misuse was alleged post-Clapper.").

[16] Falkenberg v. Alere Home Monitoring, Inc., No. 13-CV-00341-JST, 2015 WL 800378, at *3-5 (N.D. Cal. Feb. 23, 2015) (citing Cal. Civ. Code § 56.36(b)(1)).

[17] In re LinkedIn User Privacy Litig., No. 5:12-CV-03088-EJD, 2014 WL 1323713, at *5-6 (N.D. Cal. Mar. 28, 2014)

[18] In re Target Corp. Data Sec. Breach Litig., No. MDL 14-2522 PAM/JJK, 2014 WL 7192478, at *2 (D. Minn. Dec. 18, 2014).

[19] In re Target Corp. Data Sec. Breach Litig., No. MDL 14-2522 PAM/JJK, Dkt. No. 357 at 28 (D. Minn. Dec. 18, 2014).

[20] Federal Rules of Civil Procedure Rule 23(b)(3). In addition to predominance issues related to damages and causations, plaintiffs may also have trouble proving individual issues predominate when they seek to certify a nationwide class when multiple state laws are at issue. See Caroline C. Cease,

Giving Out Your Number: A Look at the Current State of Data Breach Litigation, 66 Ala. L. Rev. 395, 418 (2014) ("Due process requires that a state have 'a significant contact or significant aggregation of contacts, creating state interests, such that choice of its law is neither arbitrary nor fundamentally unfair' to subject a party to its substantive law. Thus, a district court ruling on a motion for class certification likely cannot apply only one law to the entire action and instead must consider how many states' laws will be implicated in the action and if those laws conflict in a way that defeats predominance.). This could be what the Target plaintiffs were referring to when they stated it could be difficult to certify the class "particularly since [Plaintiff's] claims are anchored in state statutory and common law claims."

[21] Comcast Corp. v. Behrend, 133 S. Ct. 1426, 1433 (2013).

[22] Id. at 1432 (internal quotation marks and citations omitted).

[23] Id. at 1433.

[24] See, e.g., Roach v. T.L. Cannon Corp., 778 F.3d 401, 407 (2d Cir. 2015) (citing cases from multiple circuits and stating "Comcast, then, did not hold that a class cannot be certified under Rule 23(b)(3) simply because damages cannot be measured on a classwide basis."); Leyva v. Medline Indus. Inc., 716 F.3d 510, 513 (9th Cir. 2013) (stating that "damage calculations alone cannot defeat certification").

[25] In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 293 F.R.D. 21, 30 (D. Me. 2013) (citing In re New Motor Vehicles Canadian Exp. Antitrust Litig., 522 F.3d 6, 25-26 (1st Cir. 2008) ("Plaintiffs cannot make their case without common proof of causation, and they can only prove causation through common means if their novel theory is viable; that viability in turn depends on their ability to establish—whether through mathematical models or further data or other means—the key logical steps behind their theory.")).

[26] Id. at *24.

[27] Id. at *31-33.

[28] Id. at *33.

[29] It is important to note that consumer class actions are just one of several significant sources of data breach liability that companies face today. For example, despite a cash settlement of "only" $10 million, Target has already spent approximately $250 million on its data breach. It is still fighting a separate class action brought by credit card issuers seeking to force Target to cover their costs associated with issuing replacement cards. Previously, T.J. Maxx paid credit card issuers over $40 million dollars. Additionally, most companies will suffer decreases in brand and stock value. The cost of offering free credit monitoring can cost more than $20 per person, and the cost of instituting additional internal security updates is significant. The Federal Trade Commission has been aggressively seeking penalties for breaches; AT&T recently agreed to pay it a $25 million fine. Unfortunately, the list of potential costs goes on.
