Post-Spokeo, Data Breach Defendants Can't Get Spooked: They Should Stand Up To the Class Action Plaintiff Boogeyman

by Marcello Antonucci, Kimberly Horn, Michael Phillips, and Bonnie Wise

This article was a collaborative effort between the following authors:

Marcello Antonucci *can be reached at Marcello.Antonucci@beazley.com*

Kimberly Horn *can be reached at kimberly.horn@beazley.com*

Michael Phillips *can be reached at michael.phillips@beazley.com*

Bonnie Wise *can be reached at bwise@wileyrein.com*

The Supreme Court could have completely altered the landscape of consumer privacy and data breach class action lawsuits in *Spokeo, Inc. v. Robins*, a closely watched case before the Court last term. Although the underlying dispute in *Spokeo* involved an alleged violation of the Fair Credit Reporting Act and not a data breach, the case presented a nagging question in privacy law: What kind of injury is sufficient for Article III standing? While the law in data breach litigation in our electronic age continues to develop, plaintiffs increasingly can expect their claims to be dismissed for lack of standing if they are unable to credibly allege some sort of actual injury, as opposed to a mere increased risk of some hypothetical future harm, and that the injury is traceable to the theft of their data from the defendant.

When the Court finally ruled in May, it did not decisively answer the question. Instead, the Court remanded the case to the Ninth Circuit, holding that the appellate court had failed to consider whether the alleged injury in fact was concrete, and instead considered only whether it was particularized. While the Supreme Court reiterated the threshold test for analyzing standing, it failed to signal whether the alleged injury actually met the applicable standard or offer any definitive statement that could tilt the playing field toward plaintiffs or defendants. In its opinion, the *Spokeo* Court defined a concrete injury as "de facto; that is, it must actually exist," but it also said that this does not mean the injury must be "tangible." These soft guideposts on standing have created a sort of Rorschach test, with both plaintiffs and defendants contending that *Spokeo* compels a decision in their favor.[1] This is especially so in the context of data breach class actions.

Since the Supreme Court issued what many view as an incomplete opinion in *Spokeo*, lower courts will continue to reach diverging conclusions as to whether data breach plaintiffs have alleged sufficient injury to proceed to the merits. This presents a difficult choice for data breach defendants who lose motions to dismiss on standing: Should they proceed to litigate the merits of such an action, which, with the exception of challenging the merits of the pleadings by way of a 12(b)(6) motion (or its state court equivalent) is uncharted territory, or should they relent, and settle? The latter can be hard to stomach, especially where the plaintiffs do not seem to have suffered any real harm.

Data breach defendants don't need to give in. Instead, they should force plaintiffs to establish their damages, and then use creative ways to approach settling these cases that simultaneously offer plaintiffs tangible benefits and reassure defendants that they are not surrendering to plaintiffs who were not, in fact, injured.

Data breach settlements differ starkly from the classic class action settlement model, in which a large fund is divided evenly among class members who opt in (or who do not opt out). Many of these settlements involve tiered settlement funds, credit and identity monitoring product offerings, data security enhancements, detailed claims processes and other settlement features that provide the parties an opportunity to avoid further litigation while also addressing many of the concerns of both plaintiffs and defendants. Here we examine the publicized details of 19 consumer data breach class action settlements to determine how litigants are resolving these disputes and what tools parties can use reach a creative compromise.[2]

The Bottom Line

When details of a privacy class action settlement are publicized, the headline tends to be the dollar amount the defendant is going to pay into a settlement fund for the class. We looked at those numbers when averaged based on the number of class members. Of the settlements we analyzed, the average amount paid per-class member ranged from $0, in *In re Adobe Systems Inc. Privacy Litigation*, to $13.63 per person, in *Rowe v. Unicare Life & Health Insurance Co. et al.* In most cases, these averaged numbers do not match the amounts actually paid to class members, because the amounts paid differ based on variables in the settlement structure, as discussed further below. Still, analysis of the fund amount per-person is useful to gauge generally how much defendants are paying in relation to the size of the class.

The data suggests that a number of variables can drive the per-person dollar amount of the settlement fund – the type of data potentially exposed, the manner in which it was exposed, the jurisdiction in which suit was brought, and the other relief provided in the settlement. For example, the per-person amounts paid in settling claims for exposing personal health information ("PHI") tend to be higher than the amounts paid to settle claims for exposing personally identifiable information ("PII"), financial information, or payment card information. The amounts paid per-class member for PHI suits that we analyzed ranged from $2.50 to $13.63, while the amounts for PII, financial information or payment card information were $0.73 to $5.23 and $0.00 to $6.32, respectively.

The size of the class may also drive the per-class member settlement amount.

For example, plaintiffs may be unlikely to accept less than $1 per class member for a class of a few thousand people. In *In re Michaels Stores Pin Pad Litigation*, the company established a $600,000 fund for a 95,000-person class – an average of $6.32 per person – and also offered one year of credit monitoring, with an additional year for anyone with unauthorized charges on their accounts. On the other hand, defendants are unlikely to pay anywhere close to $1 per class member to settle an action brought by a class on behalf of 100 million potentially affected individuals. The parties have to find a sweet spot, balancing the size of the class with the realities of what a defendant should actually pay.

Plaintiffs may contend that another driver of settlement amounts is the manner in which the data was exposed. Plaintiffs believe they have more leverage to demand higher settlement amounts where the circumstances of the underlying breach allow plaintiffs to argue that the defendant was lax in its security measures. Perhaps based on this dynamic, settlement amounts based on breaches involving unauthorized physical access or the theft of unencrypted devices tend to be more costly than those based on unauthorized electronic access or hacking. For example, in *Johansson-Dohrmann v. CBR Systems, Inc.*, the defendant established a fund of $8.56 per person (a $500,000 fund for out-of-pocket losses and $2 million for identity theft, or $2.5 million, for a class of 292,000) where unencrypted backup tapes containing PII and financial data were stolen from an employee's car. The average settlement fund for the hacking incidents analyzed, on the other hand, was about $0.50 per class member.

Evidence that class members were victims of actual identity theft can also influence the settlement range – though such evidence should not automatically prompt a panicked rush to settle by the defendant. Where some plaintiffs can show actual identity theft damages, those damages may undermine the plaintiffs' ability to satisfy the commonality and predominance requirements for class certification. Moreover, as discussed further below, the settlement can be structured to compensate plaintiffs with actual identity theft damages and separately address those plaintiffs who cannot show damages. There is no magic in determining a reasonable settlement range, but as expected, the manner in which the data was exposed, the volume and type of data exposed, and evidence of actual damages are all factors relied upon by plaintiffs to assert that higher settlement amounts are warranted.

Non-Cash Benefits

The settlements with the lowest per-class member dollar amounts tend to also involve relief apart from the settlement fund – non-cash benefits such as vouchers for customers, credit monitoring or identity monitoring services, or clearly delineated security enhancements that the defendant must undertake.

The data shows that the most common of the non-cash settlement elements is credit or identity monitoring. Incorporating those costs into a proposed settlement presents some challenges, however. Many defendants will already have offered and paid for credit or identity monitoring to a large number of class members in initially responding to the breach, and plaintiffs, their counsel, or the court in considering the settlement may be unwilling to consider that prior expense as part of the settlement. Some companies have tacked on additional years of credit monitoring as part of the settlement or re-opened the offer of monitoring to class members who did not opt in the first time around. While credit monitoring can be useful depending on what type of data has been exposed, plaintiffs and their counsel may not place a high value on offering it as part of a settlement package because those class members who were interested in such an offering have typically already enrolled following public notification of the breach. Still, it is one clear way to provide a non-cash benefit to compensate all those potentially affected by the breach.

Network security enhancements may present the most clear-cut way to benefit all parties to data privacy class actions. Defendants strengthen their systems in an effort to avoid future similar incidents (and the risk of liability that flows from them), and plaintiffs gain further protection for data that the company may still possess or may obtain in the future. This is particularly useful where a number of class members are likely to do business with the defendant company in the future.

The *Target Corp.* settlement, for example, incorporated security measures that Target agreed to adopt, including designating a high-level chief information security officer to oversee information security programs, maintaining written information security programs, maintaining a process to monitor

continued on page 15

Data Breach Defendants continued from page 5

for information security events and respond to threats, and educating and training relevant employees regarding the importance of securing consumers' PII. The Adobe settlement also mandated specific security enhancements, the details of which were largely redacted from the settlement documents to maintain their effectiveness in fending off future hackers. The settlements in *Curry v. AvMed Inc.* and *Burrows v. Purchasing Power LLC* also featured detailed security improvements, and in the *Heartland Payment Systems Inc.* settlement, the defendant agreed to report to an expert selected by the plaintiffs regarding its remedial measures. The finality of the *Heartland* settlement was conditioned on the plaintiffs' expert's acceptance of the report.

While negotiating these details and involving security experts in the settlement process can take time and increase the cost of reaching a settlement, it can also create a path to provide real value to the plaintiffs while still accounting for the defendant's views that the breach at issue did not cause the plaintiff's actual injury. The settling parties often quantify in dollars the amount the defendant will spend on security investments, so that the court evaluating the settlement can consider it as a component of the overall settlement value.

The Claims Processes

A final area where privacy class action litigants have developed innovative solutions is in structuring how the settlement fund is paid out to class members. As noted, these class actions do not tend to follow a model in which the total fund is divided evenly among class members who opt in to the settlement. Instead, these settlements feature carefully constructed procedures in which class members submit claims and seek reimbursement from the fund. In some cases, the class members must submit a certification or proof of losses with their claim for reimbursement from the fund. The *Target* settlement, for example, allowed two types of claims – documentary claims or self-certification claims. Class members who submitted documents showing out-of-pocket loss could be reimbursed up to $10,000, while class members submitting only self-certifications were entitled only to an equal share of the amount remaining after all documentary claims were paid out (estimated beforehand to be roughly $40 per person). This claims process smartly prioritizes payments to class members who have suffered out-of-pocket losses over class members whose harm is merely speculative (or virtually non-existent).

The *AvMed* settlement followed a similar pattern – approved identity theft claims would be paid first, then the remainder would be divided among "premium overpayment claims." Prior to the *AvMed* settlement, however, the Eleventh Circuit had found that even class members who had not been victims of identity theft had sufficiently pled injury by claiming that they paid more in premiums in exchange for AvMed sufficiently protecting their data. While this precedent may explain the why the parties in *AvMed* adopted this approach, distinguishing between plaintiffs with real damages and those without is sensible even where the court has made no such ruling.

Another innovative approach is setting up a settlement fund with payment tiers, such that the second tier only comes into play if enough class members submit valid claims to exhaust the first tier. The parties to the *Heartland* settlement agreed to a $1 million settlement fund, but if valid claims exhausted that fund, Heartland would contribute up to another $1.4 million. This approach strikes a balance between the plaintiffs' interest in seeing that defendants make some payment to compensate for the breach, and in particular, that it compensate class members who have suffered actual harm, as well as the defendants' interest in limiting the amounts they pay to compensate for hypothetical and speculative harm.

Put another way, if the plaintiffs are right that the class has suffered and can prove real harm, the settlement is designed so that the defendant will compensate for that harm. On the other hand, if the defendant is right that many (or most) class members have no actual injury, then the defendant will not have to pay the higher tiers of the fund. In this way, the settlement incorporates both sides' views of the merits but also limits the risk for both sides that proceeding to litigation would entail.

Conclusion

While post-*Spokeo* courts may continue to issue inconsistent opinions, the environment for data breach defendants is not as frightening as it appears. Defendants should relentlessly challenge plaintiffs to justify their alleged grievances and establish their damages. Efficient solutions such as credit and identity monitoring services for the truly affected can mitigate the risk of larger and consequential damages. Creatively structured settlements such as the "tiered" approaches described above put the onus on the plaintiffs to prove their damages–which, as one court approving such a settlement has noted, they would have to do at some point anyway.[3] A robust claims process is key to effective settlements like these. Defendants should retain experienced privacy counsel from the first notice of a potential dispute, and incorporate sophisticated risk management solutions to make data breaches less of a nightmare.

Endnotes

1 In the wake of the *Spokeo* ruling, parties on both sides of pending class actions rushed to supplement their briefs to explain why *Spokeo* supports their arguments for or against dismissal. Barnes & Noble Inc. filed a brief in a data breach class action pending in Illinois federal court just days after the ruling, contending that the lead plaintiffs failed to demonstrate a concrete injury to satisfy the *Spokeo* standard. *In re Barnes & Noble Pin Pad Litigation*, No 1:12-cv-08617 (N.D. Ill.). On the other hand, the plaintiffs' class in a data breach suit against Paytime, Inc., in a brief filed in the Third Circuit shortly after the ruling, argued that *Spokeo* compelled reversal of the dismissal of their suit. *Storm v. Paytime, Inc.*, No. 15-3690 (3d Cir.). The Sixth Circuit Court of Appeals recently ruled that data breach plaintiffs met the standing bar established by *Spokeo*, even where they had no evidence their data had been misused. *Hancox v. Nationwide Mutual Ins. Co.*, No. 15-3387 (6th Cir.).

2 The data breach class action settlements analyzed were: *In re Adobe Syst. Inc. Privacy Litig.*, No. 13-5226 (N.D. Cal.); *In re Heartland Payment Syst., Inc. Data Security Breach Litig.*, No. 09-2046 (S.D. Texas); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. 11-2258 (S.D. Cal.); *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522 (D. Minn.); *In re TJX Cos. Retail Security Breach Litig.*, No.07-10162 (D. Mass.); *In re The Home Depot Inc. Customer Data Sec. Breach Litig.*, No. 14-02583 (N.D. Ga.); *In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig.*, No. 08-1998 (W.D. Ky.); *Beringer v. Certegy Check Servs., Inc.*, No. 8:07-cv-01657 (M.D. Fla.); *In re Dep't of Veterans Affairs Data Theft Litig.*, No. 06-506 (D.D.C.); *Lim v. Vendini Inc.*, 1-14-CV-259897 (Cal. Super. Ct., Santa Clara Cnty.); *In re LinkedIn User Privacy Litig.*, No. 12-3088 (N.D. Cal.); *Rippy v. Schnuck Markets Inc.*, No. 2013-L-218 (Ill. Cir. Ct., St. Clair Cnty.); *Curry v. AvMed Inc.*, No. 10-24513 (S.D. Fla.); *Burrows v. Purchasing Power LLC*, No. 12-22800 (S.D. Fla.); *In re Michaels Stores Pin Pad Litig.; Johansson-Dohrmann v. CBR Systems, Inc.*, No. 12-1115 (S.D. Cal.); and *Rowe v. Unicare Life & Health Ins. Co.*, No. 09CH05166 (Ill. Cir. Ct., Cook Cnty.)

3 *In re Countrywide Financial Corp. Customer Data Security Breach Litigation,* No. 08-1998 (W.D. Ky.), Docket No. 297, at 9 ("Perhaps Plaintiffs' two biggest challenges are the issues of causation and damages, both of which are essential to maintaining a successful case. Moreover, the current state of the law in regards to data breaches does not bode well for Plaintiffs. For these reasons, the Court believes this factor weighs heavily in favor of settlement.")