February 2015

Weil

Class Action Monitor

The Next Frontier in Data Breach Notification: Federal Legislation and State Law Preemption

By David R. Singh and Meredith Santana

In This Issue

Target, Home Depot, Anthem, and Neiman Marcus are but a few of the major companies that have recently made headlines for large-scale data breaches involving the personal information of millions of consumers. Though unique in their scale, these high-profile security breaches are, unfortunately, no longer an anomaly. The frequency and magnitude of data breaches continue to increase. In response, most states have enacted data breach notification laws that prescribe procedures for businesses to notify consumers about significant disclosures of sensitive personal information. The result has been a patchwork of conflicting state laws that make compliance costly for businesses operating across multiple states. Previous efforts at enacting federal legislation to supersede state notification laws have repeatedly stalled. However, a recent proposal by President Barack Obama appears to have reinvigorated efforts to enact a national data breach notification standard, and congressional hearings to develop a federal statute are already underway. Although the enactment of a federal notification standard has the potential to alleviate the burden of regulatory compliance for national businesses, the extent to which it does so will depend on whether the federal legislation preempts state notification laws or forecloses enforcement under other applicable state statutes.

State Notification Statutes

To date, 47 states have enacted data breach notification laws.[1] Only three states have yet to enact notification statutes: Alabama, New Mexico, and South Dakota.[2] Most state notification laws follow the same general structure and require businesses to provide prompt notice of a security breach to affected individuals and often the state attorney general, a designated state agency, or consumer reporting agencies. However, there is significant variation among the state laws. Under California's data breach law, which has served as the model for several other states, businesses must notify individuals of any breach of unencrypted personal data "in the most expedient time possible and without unreasonable delay."[3] Other states impose a specific time frame and require notice to be made within 30 to 45 days.[4] Notably, not all data breaches trigger state notification requirements.

In the aftermath of recent large-scale breaches, states have rushed to further tighten existing requirements. Legislators in Target's home state of

Minnesota, for instance, proposed an amendment that would have required businesses to provide notice within 48 hours of discovery of a security breach and to reimburse customers for any fraudulent expenses incurred as a result of a breach.[5] Florida successfully shortened its notification period from 45[6] days to 30 days.[7] And, in New York, Attorney General Eric Schneiderman is currently backing legislation that would broaden the definition of "personal information" under the state's data breach notification statute.[8]

Federal Legislation

For years, many have called for federal legislation to replace incongruous state laws with a national notification standard. A federal data breach notification statute would not only give national businesses a uniform set of requirements to follow, thereby making compliance easier and less expensive, but it would also extend federal protection to individuals in the three remaining states without data breach statutes. Despite the advantages of federal legislation, attempts at enacting federal legislation have been controversial, particularly with respect to the issue of federal preemption of state law. For example, state attorneys general, who are often empowered by state data breach notification laws, have resisted legislation that would preempt stringent state notification requirements.[9]

Since 2013, federal lawmakers have unsuccessfully introduced at least five proposals for data breach notification legislation that would have preempted state law. Bills proposed by Senator Patrick Leahy,[10] Senator Jay Rockefeller,[11] and Senator Richard Blumenthal[12] would have preempted state data breach notification laws while granting enforcement authority to state attorneys general. A bill by Senator Pat Toomey would have gone a step further to preempt not only data breach notification laws but also any law pertaining to the security of personal data.[13] Meanwhile, a bill by Senator Tom Carper would have preempted all state action, including any notification laws as well as any law intended to protect the security of consumer data, safeguard data from misuse, or mitigate the harm resulting from security breaches.[14] To date, none of the five bills has been reported out of committee.

President Obama's Proposal

After years of failed proposals, however, there appears to be new momentum to enact a comprehensive federal data breach statute. On January 13, 2015, President Obama announced a proposal for federal data breach legislation that largely draws upon previous legislative proposals. Under the Personal Data Notification & Protection Act, business entities that store "sensitive personally identifiable information" of more than 10,000 individuals would be required to provide notification of security breaches without "unreasonable delay," currently defined as fewer than 30 days.[15] Businesses would be able to delay notice to affected individuals if they were able to prove that additional time is "reasonably necessary" to assess the scope of the breach or prevent additional disclosures.[16] In addition to providing notice to affected consumers, business entities would be required to provide notice to an agency to be designated by the Secretary of Homeland Security when more than 5,000 individuals are affected by any particular breach.[17] The law would also provide several exemptions to the notice requirement. Under the national security and law enforcement exemption, no notice would be required if the Secret Service or FBI determine that notification might "reveal sensitive sources" or the FBI determines that providing notice "could be expected to cause damage to the national security."[18] Under the safe harbor provision, a business would be exempt from providing notice if it conducts a risk assessment and determines there is "no reasonable risk that a security breach has resulted in, or will result in, harm to affected individuals."[19] Finally, under the financial fraud prevention exemption, a business would be exempt if it utilizes a security program that "effectively blocks the use of sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual."[20]

As the proposal progresses through the House and Senate, amendments to two key provisions will be of particular importance to businesses that engage in interstate commerce: the 30-day notification requirement and the state law preemption provision. The 30-day notification requirement has been

criticized because it imposes a stricter time frame than most state statutes and because it would limit the amount of time available for businesses to investigate a breach. As currently formulated, the federal statute would supersede any state law "relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data."[21] The law would also grant state attorneys general authority to bring suit to enjoin any practice that does not comply with federal requirements, to enforce compliance, and to impose penalties of up to $1,000 per day per violation.[22] However, the preemption provision has already been the subject of much debate and may be amended in an effort to build consensus in favor of the legislation. At a recent hearing held by the Commerce, Manufacturing, and Trade Subcommittee of the House Committee on Energy and Commerce to discuss the elements of a federal data breach statute, the question of federal preemption was a central point of disagreement.[23] Therefore, although President Obama's proposal provides a template for a future federal statute, the details of the notification requirement and the extent to which the legislation would preempt state data breach notification laws remains unclear. We will continue to monitor the progress of President Obama's proposal for a federal data breach notification law and will provide updates as to its status and these open issues.

1. *Security Breach Notification Laws*, National Conference of State Legislatures (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
2. *Id.*
3. Cal. Civ. Code § 1798.82 (a) (2015).
4. *See, e.g.*, Fla. Stat. § 501.171(4)(a) (2014) (requiring notice no later than thirty days); Ohio Rev. Code Ann. § 1349.19(B)(2) (2007) (requiring "notice in the most expedient time possible but not later than forty-five days").
5. *See* H.F. 2253, 88th Leg. (Minn. 2014).
6. *See* Fla. Stat. § 817.5681 (repealed 2014).
7. *See* Fla. Stat. § 501.171(4)(a) (2014).
8. Press Release, Office of Attorney General Eric T. Schneiderman, A.G. Schneiderman Proposes Bill To Strengthen Data Security Laws, Protect Consumers From Growing Threat Of Data Breaches (Jan. 15, 2015), *available at* http://www.ag.ny.gov/press-release/ag-schneiderman-proposes-bill-strengthen-data-security-laws-protect-consumers-growing.
9. *See, e.g., Protecting Consumer Information: Can Data Breaches Be Prevented? Before the H. Subcomm. on Commerce, Manufacturing, and Trade Committee on Energy & Commerce*, 113th Cong. (2014) (statement of Lisa Madigan, Attorney General of Illinois), *available at* http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-MadiganL-20140205.pdf.
10. Personal Data Privacy and Security Act of 2014, S.1897, 113th Cong. (2014).
11. Data Security and Breach Notification Act of 2014, S.1976, 113th Cong. (2014).
12. Personal Data Protection and Breach Accountability Act of 2014, S.1995, 113th Cong. (2014).
13. Data Security and Breach Notification Act of 2013, S.1193, 113th Cong. § 6 (2014).
14. Data Security Act of 2014, S.1927, 113th Cong. § 7 (2014).
15. Personal Data Notification & Protection Act § 101(c) (2015) (as proposed by President Barack Obama).
16. *Id.*
17. *Id.* at § 106(a).
18. *Id.* at § 102(a)(1).
19. *Id.* at § 102(b).
20. *Id.* at § 102(c)(1).
21. *Id.* at § 109.
22. *Id.* at § 108(a)(1).
23. *See Hearing on What Are the Elements of Sound Data Breach Legislation? Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Energy and Commerce Comm.*, 114th Cong. (2015) (statement of Brian A. Dodge, Retail Industry Leaders Association) (calling for a "carefully crafted federal data breach law has the potential to clear up regulatory confusion, remove conflicting rules, and better protect and notify consumers.").

Effective Discovery Strategies in Class Action Litigation

By David R. Singh and Gaspard Curioni

Discovery in class action litigation is notoriously asymmetric. While a corporate defendant may have hundreds of thousands or millions of potentially relevant documents dispersed geographically and across a range of systems, the putative class representative is likely to have a relatively small number of responsive documents, which can be collected and produced with little burden or expense. Accordingly, corporate defendants in class actions are vulnerable to attempts by plaintiffs to propound extremely broad discovery requests, in the hopes that driving up the expense of the litigation will force the defendant to settle regardless of the merits of the case (or the lack thereof). This article discusses various strategies for combating this common tactic and reining in the expense of discovery in class action litigation.

A. Discovery Stays Pending Motion to Dismiss

At the start of a putative class action, defense counsel should consider seeking a stay of discovery while a motion to dismiss is pending. Courts stay discovery at their discretion, *see* Fed. R. Civ. P. 26(c)(1)(A), usually by balancing the relative harms between plaintiffs and defendants. *See, e.g., Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1996 WL 101277, at *2-3 (S.D.N.Y. Mar. 7, 1996). The balance of harms should typically tilt in a defendant's favor. On the one hand, the harm to the defendant is likely to be significant. Discovery costs are potentially immense in class actions, given, among other things, the costs associated with collecting and reviewing electronic information, the storage of electronic information across a multitude of systems, the dispersal of hard documents in different sites in various geographic regions (including potentially overseas), the need to retrieve documents from offsite storage, and the need to collect documents related to thousands or millions of transactions. Defendants should not be subjected to these significant expenses if the putative class action complaint is unlikely to survive a motion to dismiss. On the other hand, the harm to the named plaintiff is often only slight. Discovery is typically unnecessary to decide a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6), and the risk of spoliation of potentially relevant documents is usually remote and easily avoidable with an appropriate document preservation order. Furthermore, where a class action challenges a longstanding business act or practice, rather than newly implemented conduct, a plaintiff generally cannot justify a sudden and urgent need for discovery.

B. Limits on the Scope of Precertification Discovery

If the court refuses to stay discovery or denies the motion to dismiss, defense counsel should consider attempting to limit the scope of precertification discovery to class certification issues. Bifurcation between merits and class certification discovery oftentimes creates efficiencies. In the typical class action, merits discovery requires a defendant to produce tens of thousands of pages of documents and to make dozens of witnesses available for depositions. This is, of course, costly. A corporate defendant should argue that it should only have to bear this significant expense if the suit is viable as a class action – that is, only once it has been certified. *See Manual for Complex Litigation (Fourth)* [hereinafter *Manual*] § 21.14 (2004). Merits discovery, moreover, could delay the certification decision, contravening the requirement that a class certification determination be made at "an early practicable time." Fed. R. Civ. P. 23(c). Aside from efficiency considerations, bifurcation is also fairer to defendants. Onerous merits discovery may pressure defendants to settle even if plaintiffs' allegations lack merit. Cases where the defendant has strong arguments against class certification, therefore, are good candidates for bifurcation. *See Manual* § 21.14; *Gonzalez v. PepsiCo, Inc.*, No. 06-2163, 2007 WL 1100204, at *3 (D. Kan. Apr. 11, 2007).

C. Shifting Precertification Discovery Costs

Defense counsel should also consider seeking to

shift precertification discovery costs to the plaintiff. In *Boeynaems v. LA Fitness Int'l, LLC*, a federal district court held that cost shifting was warranted in certain putative class actions. 285 F.R.D. 331, 334-35, 341 (E.D. Pa. 2012). The plaintiffs in that case had signed up to join a health club but allegedly encountered obstacles when they sought to terminate their membership. They filed a putative class action and propounded extremely broad and burdensome discovery requests on the defendant. In the court's assessment, the parties faced "asymmetrical" discovery burdens: the plaintiffs had "very few documents" compared to the defendant's "millions of documents and millions of items of electronically stored information." *Id.* at 334. If the plaintiffs had their way, the defendant would bear the brunt of "[v]irtually all" of precertification discovery at a cost that constituted "a significant factor in the defense of the litigation." *Id.* As the court observed, although a responding party usually bears the costs of discovery requests, the court can shift the costs to the plaintiffs if the requests are unduly burdensome. Applying this principle to the putative class action context, the court held that cost shifting is proper in cases where (1) "class certification is pending," and (2) the discovery requests are "very extensive" and "very expensive," unless there are "compelling equitable circumstances to the contrary." *Id.* at 341. In reaching this conclusion, the court reasoned that "*discovery burdens should not force either party to succumb to a settlement that is based on the costs of litigation rather than the merits of the case*." *Id.* at 342 (emphasis added). The court also discussed the economic pressures faced by class action defendants. In the instant case, since the defendant had "borne all of the costs of complying with Plaintiffs' discovery to date," the court ruled that the plaintiffs should pay for any "additional discovery." *Id.* at 341. Accordingly, there is persuasive precedent for shifting the cost of precertification discovery to the plaintiff. At the very least, the precedent provides a credible basis for threatening to file a cost-shifting motion if the plaintiff does not withdraw or narrow his or her unreasonable discovery requests. *See also Schweinfurth v. Motorola, Inc.*, No. 1:05CV0024, 2008 WL 4449081, at *2 (N.D. Ohio Sept. 30, 2008) (splitting precertification discovery costs evenly between the parties).

D. Precertification *Daubert* Challenges

It has become increasingly common for plaintiffs to proffer expert testimony at the class certification stage to establish that the requirements of Rule 23 have been satisfied. Even where the expert's report overlaps with the merits of the case (such that the expert is likely to submit another report during the merits stage of the case), defense counsel should not wait to challenge the admissibility of the expert's testimony. If the defendant does not act, the plaintiff may argue that the defendant has waived its right to challenge the admissibility of the testimony under Fed. R. Evid. 702. The standard for testing expert reliability at the class certification stage remains unsettled, however. Some circuits require a full-blown *Daubert* analysis on the view that expert testimony leading to certification could be outcome determinative: once a class is certified, defendants are under intense pressure to settle. *See Sher v. Raytheon Co.*, 419 F. App'x 887, 890-91 (11th Cir. 2011); *Am. Honda Motor Co. v. Allen*, 600 F.3d 813, 815-16 (7th Cir. 2010); *cf. Unger v. Amedisys Inc.*, 401 F.3d 316, 323 n.6 (5th Cir. 2005) (suggesting that courts may inquire into the admissibility of an expert's testimony at the certification stage). Other circuits arguably require a more focused *Daubert* test on the theory that reliability is a function of the available information and that experts have access to limited information at the certification stage. *See Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 982 (9th Cir. 2011); *Cox v. Zurn Pex, Inc.*, 644 F.3d 604, 612-614 (8th Cir. 2011). The Supreme Court has left this circuit split unresolved, but the high court has suggested in dicta that a full-blown *Daubert* analysis may be required. *See Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2554 (2011); *Comcast v. Behrend*, 133 S. Ct. 1426, 1432 (2013). Given the unsettled state of the law and the logic of not certifying a class based on unreliable expert testimony, defense counsel should argue that rigorous analysis of certification issues requires a thorough assessment of experts' reliability akin to a full-blown *Daubert* inquiry. *See In re Hydrogen Peroxide Antitrust Litig.*, 552 F.3d 305, 323 (3d Cir. 2009).

E. Limiting Discovery Concerning Unnamed Class Members

In an attempt to impose a burden on defendants and/or to recruit new or additional plaintiffs, plaintiff's counsel often seek discovery about unnamed class members. Defense counsel should counter such attempts. The rules for discovery of unnamed class members are stricter than the general discovery regime: the named plaintiff must demonstrate that the information is needed for certification. *Manual* § 21.14. Further, discovery may be limited to "a certain number or a sample of proposed class members." *Id.* Additionally, subject to the First Amendment, courts may limit communications from plaintiff's counsel with potential class members in order to prevent abuse and ethical violations. *See Hauff v. Petterson*, No. 1:09-cv-00639, 2009 WL 4782732, at *32 (D.N.M. Dec. 11, 2009). Some courts have gone further and restrained plaintiffs from discovering information from defendants *about* potential class members to protect privacy rights. Under the opt-in approach, plaintiffs cannot obtain information relating to unnamed class members from defendants unless the concerned individuals consent. *Best Buy Stores, L.P. v. Superior Court*, 40 Cal. Rptr. 3d 575, 577 (Cal. Ct. App. 2006). Under the opt-out approach, the presumption is reversed: plaintiff may obtain information about unnamed class members unless the latter parties object. *Pioneer Elecs. (USA), Inc. v. Superior Court*, 150 P.3d 198, 205-06 (Cal. 2007). Either approach is more protective than the unchecked release of private customer information.

F. Targeted Precertification Depositions

Depositions of named plaintiffs at the certification stage give defendants an early opportunity to discover facts that undermine plaintiffs' theories of classwide harms. In deciding who to depose first, defense counsel should target the "weakest links" to lock in damaging testimony before plaintiff's counsel have had an opportunity to coach witnesses and adjust their legal theories. Identifying promising targets might require running background checks on the named plaintiffs, retrieving their consumer records, and sweeping social media for damaging comments. Factors to consider include the named plaintiff's criminal record, the existence of class action waivers (common in credit card agreements and online terms of use), the named plaintiff's public comments on the pending litigation, and whether the named plaintiff is a serial litigant or is related personally or professionally to plaintiff's counsel (as is often the case because consumer class actions are often driven by plaintiff's counsel who conceive of a legal theory and then recruit individuals to serve as class representatives to prosecute them). Priority should be given to taking early depositions in the cases in which the stakes are the highest.

Conclusion

Discovery stays, motions to bifurcate, and cost shifting motions are powerful tools for reducing discovery costs in putative class actions and forcing a resolution that is reflective of the merits of the case, rather than the cost of litigation. At the same time, it is often well worth the investment to take some focused discovery early, including by taking targeted depositions, to expose the weakness of plaintiff's case (and thereby influence the settlement dynamic), and to oppose class certification. By incorporating defensive and offensive elements into their discovery strategy, defense counsel can lay the foundation for timely, fair, and cost-efficient resolution of a putative class action.

A prior version of this article was published in the Spring 2014 edition of Corporate Counsel, the newsletter of the American Bar Association Section of Litigation Corporate Counsel Committee.

Class Action Monitor is published by the Litigation Department of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue of *Class Action Monitor*, or would like more information about Weil's Class Action practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editor:

David R. Singh	Bio Page	david.singh@weil.com	+1 650 802 3010

Contributing Authors:

Gaspard Curioni	Bio Page	gaspard.curioni@weil.com	+1 212 310 8068