AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

Mediation Matters

By John G. Loughnane

The Role of Resolution in Resiliency

John G. Loughnane
Nutter McClennen & Fish LLP; Boston

John Loughnane is a partner with Nutter McClennen & Fish LLP in Boston.

Efficient resolution of disputes arising from a data breach should form part of a resilient company's response strategy. This is especially true for small- and medium-sized businesses with (1) limited resources, and (2) less time for prolonged disputes.

The general topic of using mediation to help resolve data breach-infused disputes was explored previously in the *ABI Journal*.[1] As noted in that article, just as mediation has been used successfully by parties to resolve issues surrounding the sale of personally identifiable information (PII), mediation can help in resolving a variety of disputes arising when a breach occurs.

Prudent companies exercise extreme care when generating, using, sharing and storing digital data. Unfortunately, the prospect of a breach can never be eliminated. This article begins with a short summary of the ongoing attacks on data, then moves on to discuss two key aspects of deploying mediation in data breach disputes: identifying key interests at stake, and exploring possible options to satisfy those interests.

Data Under Attack

A range of attackers deploy a host of nefarious activities in the pervasive effort to pilfer data. In addition to outside threats, data is also at constant risk from disgruntled employees or simple insider inadvertency or negligence. Cybercrime represents a growing and serious threat to businesses of all sizes. The World Economic Forum's 2016 Global Risk Report indicates that cybercrime cost the global economy $445 billion in 2014 alone.[2] The security challenge is aptly captured in this oft-repeated remark: "[T]here are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[3]

This modern-day reality does not mean that companies are powerless to defend against a breach, but it is quite the contrary. For all of the notable breaches that have occurred, significant investment and diligence have effectively prevented or reduced the impact of countless others. Successful security is the result of concentrated efforts by companies to build and nurture secure environments as a matter of business necessity — mandated by various regulations, trading partners and internal governance. Successes do not receive public acclaim, but they are the reason that many businesses flourish in the digital age and consumers enjoy the modern-day conveniences of one-click shopping and next-day delivery.[4]

However, data breaches continue to proliferate. Although one breach alone may not topple a company, a poor response to a breach can imperil the financial health of the breached company or third parties that entrusted data to that company. Unfortunately, small- and medium-sized businesses are just as prone to attack as major companies with familiar names. Moreover, smaller entities often lack a sufficient information-technology infrastructure to guard against the newest attacks.

Numerous well-publicized breaches have resulted in a flurry of litigation and helped shape corporate-response protocols. Many large companies that have exposed PII have endured reputa-

1 John G. Loughnane, "Mediating Cybersecurity Disputes in Distressed Circumstances," XXXVI *ABI Journal* 7, 26-27, 47, July 2017, *available at* abi.org/abi-journal (unless otherwise specified, all links in this article were last visited on Nov. 20, 2017).

2 "The Global Risks Report 2016, 11th Edition," World Economic Forum, *available at* www3.weforum.org/docs/GRR/WEF_GRR16.pdf.

3 Robert S. Mueller, III, Remarks Prepared for Delivery to the RSA Cyber Security Conference, San Francisco, March 1, 2012, *available at* archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

4 Corporate data security is a complex topic well beyond the scope of this article. A good guide to security principles is maintained by the National Institute of Standards and Technology (NIST) through its Framework for Improving Critical Infrastructure Cybersecurity (commonly known as the Cybersecurity Framework). The core of the voluntary framework consists of five functions intended to be implemented concurrently and continuously: identify, protect, detect, respond and recover. A copy of the Cybersecurity Framework, which is currently in the process of being updated by NIST, is available at nist.gov/cyberframework.

tional injury and some financial harm, but have survived the ordeal. Companies with well-designed response playbooks deployed strategic plans, including notifications to appropriate authorities, affected parties and insurers, as well as additional steps. Financial exposure has been softened in many cases by applicable insurance coverage or court decisions refusing to reward damages for disclosure of PII alone without some more particularized injury.[5] Although best practices have developed for responding to a data breach (especially breaches involving PII) and the losses incurred to date have been absorbed in many cases, there are at least two reasons to be prepared for an increase in the ramifications of data breaches moving forward.

First, the Equifax data breach, which impacts approximately 145.5 million U.S. citizens, has helped fuel public concern about cybersecurity.[6] As a result, Congress or state legislatures might coalesce around new penalties or consequences for insufficient data security. Moreover, the U.S. Supreme Court may elect to take up the question of standing for those alleging future harm arising from a data breach that could increase damage exposure.[7]

Second, the amount of sensitive information maintained by a company in digital form extends well beyond PII — and this is true for companies of all sizes. In a recent study, the Ponemon Institute identified small- and medium-sized businesses that are focused on protecting customer records, business correspondence, employee records, financial information and intellectual property.[8] In short, with the amount of digital corporate data growing quickly across businesses of all sizes, the consequences of a successful attack increases exponentially for the company that is breached, as well as any party entrusting its information to the breached party.

In short, the magnitude of the attack on data of all types (including PII) cannot be overstated. Although one breach alone may not trigger corporate distress, it certainly has in the past and will in the future for some challenged companies.[9] Failure to respond to all aspects of a breach effectively only compounds the risk. In any setting, a successful mediation depends on identifying the key interests at stake, as well as options to satisfy those interests.

Interests at Stake

The key interest of a company affected by a data breach will be in responding and recovering from the breach as quickly and efficiently as possible. Response and recovery will often require interaction with multiple third parties depending on the circumstances: customers, vendors, insurers, regulators, partners and others. Whether the interests of such parties are addressed out of court or with the benefit of a breathing spell afforded by a formal reorganization process, efficient resolution is essential. Interests of commercial parties will vary but will surely include confirmation that the specific cause of the breach has been identified and remedied, that the costs of collateral damage created by the breach are covered, and assurances that changes are implemented to reduce the risk of similar breaches in the future.

When a breach occurs, mediation offers a means for resolving the resulting disputes. Companies ... can preserve value by dealing with data-breach disputes efficiently.

In the case of consumers or employees affected by an attack on PII, the universe of those alleging harm might be widespread. In situations of widespread harm involving PII among larger enterprises, it is not uncommon for class action lawsuits or multidistrict litigation to ensue. Unfortunately, in that situation, the reality of compensation for the plaintiffs' counsel can become an additional interest that is challenging (but not impossible) for a breached company to address.[10]

The Bankruptcy Code contains provisions to guard the interests of consumers whose PII might be sold. Specifically, the Code contains a definition of PII,[11] and requires an ombudsman to be appointed[12] and evaluation of the privacy issues in any sale.[13]

The concept of an ombudsman might be helpful as well to ensure that the interests of parties affected by a breach are being considered — whether or not PII (as defined specifically by the Bankruptcy Code) is at stake. For example, in the event of an insolvency proceeding of a consumer reporting agency that has experienced a breach, consumers will clearly have interests at stake.[14] However, the definition in § 41A of the Code would not compel the appointment of an ombudsman, as the definition of PII requires that information be "provided *by an individual* to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes."[15] Information held by a consumer reporting agency is delivered not by the consumer directly but by third parties.

5 *See Spokeo Inc. v. Robins*, 578 U.S. ___, 136 S. Ct. 1540 (2016) (holding that plaintiff bears burden of establishing standing by demonstrating, among other things, injury in fact through invasion of legally protected interest that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical").

6 The 2017 Equifax data breach was not the first suffered by the company. *See* Thomas Fox-Brewster, "A Brief History of Equifax Security Fails," *Forbes*, Sept. 8, 2017, *available at* forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#187cebe677c0.

7 On Oct. 30, 2017, a health insurer that experienced a data breach in 2014 filed a *writ of certiorari* with the Supreme Court urging the Court to resolve a circuit split on the application of *Spokeo* (*see* n.5) in data breach cases. The petition seeks review of the D.C. Circuit's Aug. 1, 2017, decision in *Chantal Attias, et al. v. CareFirst* (Case No. 16-7108), which held that the risk of future harm alleged by policyholders suing over the 2014 data breach was enough to meet the *Spokeo* standing rule.

8 The 2017 State of SMB Cybersecurity Report is available at prnewswire.com/news-releases/2017-ponemon-institute-study-finds-smbs-are-a-huge-target-for-hackers-300521423.html.

9 One example of a breach leading to a bankruptcy filing is *In re Altegrity Inc.* (Case No. 15-10226-LSS pending in the U.S. Bankruptcy Court for the District of Delaware; discussed *supra* n.1) (breach led to exposure of tens of thousands of federal employee personnel records, the cancellation of a federal contract and chapter 11 bankruptcy). Another example is *In re Impairment Res. LLC* (Case No. 12-10850-BLS also pending in the U.S. Bankruptcy Court for the District of Delaware) (theft of computer hardware containing unencrypted medical information for approximately 14,000 people led to chapter 7 for medical records firm). A significant data breach also occurred pre-petition in *In re 21st Century Oncology Holdings Inc.* (Case No. 17-22770 pending in the U.S. Bankruptcy Court for the Southern District of New York, but breach was not itself triggering cause of bankruptcy filing).

10 For example, Anthem Inc., which suffered a data breach affecting nearly 80 million people, announced a $115 million settlement to provide credit monitoring for two years to affected individuals, as well as coverage for out-of-pocket expenses. The court-approved settlement included up to $38 million in attorneys' fees — value not otherwise allocable elsewhere.

11 11 U.S.C. § 101 (41A).

12 11 U.S.C. § 332.

13 11 U.S.C. § 363.

14 Although Equifax, Experian and TransUnion are the three most widely known examples of consumer reporting agencies, many others exist in the business of collecting various types of information about consumers from third parties. The Consumer Financial Protection Bureau has compiled a list, which does not purport to be all-inclusive, of a variety of consumer reporting agencies. *See* "List of Consumer Reporting Agencies," CFPB (2016), *available at* files.consumerfinance.gov/f/201604_cfpb_list-of-consumer-reporting-companies.pdf.

15 Emphasis added.

Thus, an ombudsman would not be required under current law in the event of a proposed sale. Although not required, it might be prudent to ensure that consumer concerns are effectively advanced by the appointment of an ombudsman in the event that consumers otherwise lack a meaningful role in the proceeding.

Another major category of party commonly asserting interests in a data breach are governmental authorities such as the Federal Trade Commission, state attorneys general and various regulators. Routinely, such authorities enter into data breach settlements with companies that have suffered a breach. These settlements typically set forth the compliance obligations moving forward, including the establishment of a comprehensive information security program, protocols for security patching, obligations for network segmentation, establishment of controls over network access, and file-integrity monitoring.[16] These authorities have been active in bankruptcy proceedings concerning proposed sales of PII. Mediation can also be used to identify and seek to satisfy their interests around data-breach issues.

Even when an orderly restructuring process proves essential in light of a breach, prolonged litigation is unlikely to be in the interest of any party interested in maximizing a return or securing a solution. Mediation should prove useful to various parties, including regulatory authorities, to help maximize value, protect privacy, limit damages and reduce expense.

Options to Satisfy Interests

As previously noted, parties affected by a data breach will hold a variety of interests. The ability to realize monetary value on a claim will depend on the breached company's financial ability, including potential insurance coverage and existing or future assets. Other interests might be satisfied through non-monetary means. Mediation can be used to help identify and crystalize vital interests of various interested parties — not just positions asserted in response to a breach.

Mediation has been used outside of distressed situations to help parties reach closure on the economic consequences of a breach. For example, in the fall of 2017, a mediated settlement was preliminarily approved between current and former employees of Seagate Technology LLC and the company arising out of a 2016 data phishing attack that affected approximately 12,000 employees. In the attack, a Seagate employee forwarded PII of fellow employees to attackers, who then used the information to file fraudulent tax returns. The settlement provides each current and former employee with two years of credit monitoring and up to $3,500 for out-of-pocket expenses.[17]

Commercial parties that have agreed to detailed contractual provisions regarding data security are increasingly turning to mediation as a cost-effective means of resolving disputes concerning compliance in the ordinary course. The International Institute for Conflict Prevention and Resolution announced the creation of a cyber panel in the summer of 2017, issuing a release noting that "[w]ith attacks occurring with both greater frequency and sophistication, smart companies and their counsel are adopting proactive strategies to prevent and/or resolve cyber-related disputes in a manner that best protects operations, customers and reputation."[18] A mediated process can help simplify the process of identifying possible insurance coverage, whether it be through specifically applicable cyberinsurance, directors and officers' insurance, general commercial coverage or perhaps through crime coverage.[19]

Conclusion

When a breach occurs, mediation offers a means for resolving the resulting disputes. Companies, especially small- and medium-sized enterprises that cannot survive prolonged litigation, can preserve value by dealing with data-breach disputes efficiently. Mediation can help affected parties identify interests and explore options for satisfying those interests, which can help contain the impact of the breach and avoid collateral consequences. Simply put, resiliency requires consideration of resolution strategy as a component of an effective response to data-breach disputes. abi

Reprinted with permission from the ABI Journal, Vol. XXXVII, No. 2, February 2018.

The American Bankruptcy Institute is a multi-disciplinary, nonpartisan organization devoted to bankruptcy issues. ABI has more than 12,000 members, representing all facets of the insolvency field. For more information, visit abi.org.

16 Eric Langland, "Survey of Data Security Requirements in Multistate Breach Settlements," IAPP, *available at* iapp.org/news/a/survey-of-data-security-requirements-in-multi-state-breach-settlements.

17 *See* Shayna Posses, "Seagate Gets Initial OK for $5.7M Worker Phishing Settlement," *Law360* (Oct. 20, 2017), *available at* law360.com/cybersecurity-privacy/articles/976597?utm_source=shared-articles&utm_medium=email&utm_campaign=shared-articles.

18 *See* "CPR Launches New Cyber Panel," International Institute for Conflict Prevention and Resolution (July 17, 2017), *available at* cpradr.org/news-publications/press-releases/2017-07-17-cpr-launches-new-cyber-panel.

19 *See* Cathy Yanni, "Best Practices for Efficiently and Effectively Settling Data Breach Claims," InsideCounsel (Oct. 27, 2014), *available at* jamsadr.com/files/uploads/documents/articles/yanni_data-breach-claims_ic_2014-10-27.pdf.