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

Cyber-U

By John G. Loughnane

Data Breach Knockout: An Example of Costs and Consequences

John G. Loughnane
Nutter McClennen & Fish LLP; Boston

John Loughnane is a partner with Nutter McClennen & Fish LLP in Boston and co-chairs ABI's Mediation Committee.

Data breaches can and do occur in enterprises of all sizes and in all industries. For that reason, every company should understand and take appropriate action to mitigate its data-breach risk, yet far too many companies (including professional service firms) fail to do so.

Insufficient information about the true costs and consequences of a breach might be one cause of inadequate planning. This article strives to increase resiliency by emphasizing the need for all business leaders (and outside professionals) to come to grips with the risks presented. To drive home the point, the article discusses the significant costs and consequences experienced as a result of a data breach at one company: Retrieval-Masters Creditors Bureau Inc., a/k/a American Medical Collection Agency (AMCA).

The Reality of Data Breach Risks

Data breach headlines frequently highlight cybersecurity issues at national retailers. With their trove of personally identifiable information (PII) on millions of consumers, such companies are frequent targets. Indeed, the frequency of publicized breaches (such as those at national retailers) might lead to cybersecurity apathy or complacency by casual observers.

For example, some business leaders may believe that such breaches show the inevitability of attack and that no defense is foolproof. Under this view, the return on investment in addressing the risk might not justify the cost or distraction of worrying about the issue. The fact that so many breached retailers carry on their affairs normally after a breach — seemingly without any long-term impact — can add to the complacency.

A case in point is The Home Depot Inc., which suffered a breach several years ago that ultimately led to a settlement with regulatory authorities in November 2020.[1] The settlement resolved a multistate investigation into the exposure of the credit card information of 40 million customers. In the settlement, Home Depot agreed to resolve investigations with 46 states and the District of Columbia with a payment of $17.5 million and various commitments to improve security.[2] For a company the size of Home Depot, the breach hardly impacted viability.

Of course, very large companies are often well positioned to manage a breach through careful planning, including cybersecurity insurance, well-considered incident-response protocols, trained internal teams, and a roster of vetted outside consultants primed to respond effectively to a breach. These factors can make a real difference in controlling costs and containing risk.[3]

Smaller and mid-sized businesses may derive a false sense of comfort about risk given the perception of its limited impact on bigger firms. Unfortunately, that view is completely misplaced: Business leaders and advisors must avoid complacency at all costs. A cybersecurity breach can knock a company flat on its back permanently, quickly impose significant expense on insiders, and create burdensome challenges for affected vendors and customers.[4]

1 "Home Depot to Pay $17.5M to States over 2014 Data Breach," *Law360* (Nov. 24, 2020), *available at* law360.com/cybersecurity-privacy/articles/1332094/home-depot-to-pay-17-5m-to-states-over-2014-data-breach (subscription required to view article; unless otherwise specified, all links in this article were last visited on Jan. 26, 2021).

2 *Id.* (noting that in a separate action related to the breach, Home Depot agreed in 2017 to a settlement of $27.25 million to resolve claims of various financial institutions).

3 Favorable law has also helped limit claims of consumer plaintiffs involving PII breaches. Specifically, courts routinely deny plaintiffs "standing" to assert claims when not accompanied by sufficiently detailed allegations of injury in fact. The standing issues arise from U.S. Supreme Court precedent, including *Spokeo Inc. v. Robins*, 136 S. Ct. 1540 (2016) (holding that Fair Credit Reporting Act requires that plaintiff demonstrate concrete and particularized injury to establish standing).

4 One type of data breach risk is the potential for use of confidential information in furtherance of a business email compromise scheme. *See* Bruce Sussman, "Hedge Fund Closes Down After Cyber Attack," Secure World (Nov. 23, 2020), *available at* secureworldexpo.com/industry-news/hedge-fund-closes-after-bec-cyber-attac (discussing fatal consequences of business email compromise scheme on hedge fund company's operations).

Business leaders must not only overcome any sense of complacency, they also need to embrace cybersecurity as a business issue — and not relegate it to the realm of information technology (IT) specialists only. When cybersecurity is viewed as a business problem, it becomes clear for all in the organization that the issue requires some level of attention from everyone — including, most importantly, senior leadership. Yet despite the pervasiveness of cybersecurity challenges encountered by individuals in both their personal and professional lives, the adoption of cybersecurity best practices lags in certain fields. Certainly, firms in heavily regulated industries such as financial services have invested heavily (and compelled business partners to do so as well) to meet applicable standards.

Full-scale adoption of cybersecurity best practices has been less well embraced elsewhere, including unfortunately in certain segments of the legal profession. This point was highlighted in the 2020 survey results of the Legal Technology Survey Report conducted by the American Bar Association's Legal Technology Resource Center (LTRC).[5]

That annual survey, which collects responses from attorneys in private practice on a range of cybersecurity issues, indicates an increasing number of firms committing to cyberliability insurance policies. Yet the number is low: just 36 percent of respondents. The positive news is that the number has been steadily rising (up from 26 percent in 2017). Also increasing over the years is the number of firms with an incident-response plan (34 percent of respondents up from 25 percent in 2018).[6] As with cyberinsurance, incident-response plans are a critical element of planning effectively for a data breach. Thus, even when complacency is not an issue, organizations must build resiliency through effective strategic planning and implementation steps taken to help mitigate risk.

AMCA: From Breach to Knockout

AMCA was a debt and medical receivables collection agency focused on collecting patient receivables for various third-party clinical-diagnostic laboratories. It counted among its most valuable customers Quest Diagnostics and Laboratory Corp. of America, two large clinical laboratories. In the normal course of its business, AMCA collected and maintained PII on millions of patients, including names, home addresses, Social Security numbers, and bank account and credit card information.[7]

In recognition of the critical need to safeguard such information, AMCA invested more than $1 million to replace its legacy technology systems in 2015 with a "proprietary, server-based, network-connected system" reflecting "current technological standards, including, importantly, appropriate data security protocols."[8] Unfortunately, that investment alone did not prove sufficient to guard against a significant attack a few years later.

AMCA first learned of information indicative of a breach in March 2019 when credit card companies reported that AMCA's systems had been used to process a disproportionate amount of charges for cards later used to make fraudulent purchases with other vendors. Upon receipt of this information, AMCA retained outside consultants who confirmed the occurrence of a system hack. Disclosure of that development and the associated compromise of PII led Quest, LabCorp and other customers to terminate business with AMCA.[9]

In addition to the immediate revenue impact, AMCA began to incur the expense burden of a data breach, such as the cost of specialized IT professionals. AMCA also bore the cost of delivering notice to millions of affected patients. Other costs included a provision of credit monitoring required to be offered to patients in certain states and costs of compliance with mandates issued by payment processors.

AMCA apparently lacked cyberinsurance, which might have provided coverage for certain breach expenses. The company covered the costs instead through a loan advanced by its principal in the amount of $2.5 million, as well as company cash. AMCA also sought cost savings from a significant reduction of headcount by more than 75 percent.

By the time it sought chapter 11 relief three months after the discovery of the breach, AMCA did not believe that any reasonable prospect of reorganization existed. Rather, the purpose of the chapter 11 filing was primarily focused on attempting to control costs in responding to demands from regulators, customers and other parties resulting from the breach.

Nine months into the chapter 11 proceeding, AMCA filed a motion seeking approval of a settlement with its principal, as well as permission to dismiss the case.[10] The company reported that it was administratively insolvent and unable to afford confirmation of a liquidating plan. AMCA believed that dismissal of the case (rather than conversion to chapter 7) was in the best interests of creditors — and only possible due to the willingness of its principal to compromise the claims against the estate and provide certain additional funding if needed.

More specifically, the principal's agreement provided the estate with sufficient resources to satisfy administrative-expense claims, U.S. Trustee fees and adequate resources for record retention post-bankruptcy. In exchange, the estate agreed to provide the principal with a release of claims that the company may have against him other than any based on actual fraud or willful misconduct.

In April 2020, the bankruptcy court partially granted approval of the dismissal motion — specifically approving the settlement between AMCA and its principal and deferring any decision on the dismissal request. In August 2020, AMCA filed a motion seeking approval of a resolution with various state attorneys general.[11] In connection with that motion, attorneys general from 41 states indicated their intent to join the settlement.

5 John G. Loughnane, "2020 Cybersecurity," Am. Bar Ass'n (Oct. 19, 2020), *available at* americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity.

6 On that point, a clear disparity exists based on firm size, with 77 percent of respondents from firms of 100 or more attorneys reporting that their firms have an incident-response plan but much smaller percentages as firm size decreases (38 percent of respondents from firms of 10-49, 23 percent of respondents from firms of 2-9 and 14 percent of solo respondents). *Id.*

7 *In re Retrieval-Masters Creditors Bureau Inc.*, Case No. 19-23185-rdd, D.E. 2 at 4 (Bankr. S.D.N.Y. 2019) (*see* Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions).

8 *Id.* at 5.

9 The impact of the AMCA breach was widely reported. *See, e.g.*, Kimberly Chin, "Quest Diagnostics Says 11.9 Million Patients May Have Been Affected by Breach," *Wall St. J.* (June 3, 2019), *available at* wsj.com/articles/quest-diagnostics-says-11-9-million-patients-may-have-been-affected-by-breach-11559562193.

10 *In re Retrieval-Masters Creditors Bureau Inc.*, Case No. 19-23185-rdd, D.E. 254 at 30-31 (Debtors' Motion for Entry of an Order Pursuant to 11 U.S.C. §§ 105(a), 305(a), 349, 365(a) and 1112(b) and Fed. R. Bankr. P. 1017(a), 2002(a)(4) and 9019(a) Dismissing Chapter 11 Case and Granting Related Relief).

11 *Id.* D.E. 315 (*see* Motion for Entry of an Order Pursuant to 11 U.S.C. § 105(A) and Federal Rule of Bankruptcy Procedure 9019(A) Approving Settlement and Authorizing Form of Agreed Final Judgment Between the Debtor and Participating State Attorneys General).

As part of that settlement, AMCA agreed to enter into an agreed final judgement with participating states to allow resolution of various state claims against AMCA relating to the breach. AMCA agreed to make a total payment to the participating states in the amount of $21 million, provided, however, that actual payment of such amount was allowed to be suspended and imposed only if the company failed to comply with injunctive relief (such as mandated compliance with federal and state laws), the development and maintenance of an information security program, and the implementation of an information security program assessment. AMCA agreed to cooperate with various attorneys general, and the parties agreed to exchange releases on certain conditions.

Thereafter, the bankruptcy court entered an order approving the settlement with the participating states.[12] In December 2020, the bankruptcy court entered an order approving the dismissal of the chapter 11 case.[13]

AMCA: Costs and Consequences

With the passage of two years since the discovery of the breach and the chapter 11 case now dismissed, it is possible to summarize at least some of the costs and consequences. Costs as of the petition date for specialized IT consultants exceeded $400,000, and costs as of that date for breach notifications to millions of recipients exceeded $3.8 million.

As previously noted, AMCA apparently lacked cyber-insurance coverage and was only able to cover such costs following a loan advanced from its principal of $2.5 million shortly before the petition date. The principal then provided additional funding during the chapter 11 proceeding pursuant to a court-approved debtor-in-possession facility in the amount of at least $415,000. As a result of the administrative insolvency of the chapter 11 proceeding, the principal agreed to subordinate his claims for reimbursement (and provide certain additional funding if needed) to the extent necessary to ensure payment of administrative expense priority claims in the case.

Administrative claims consisted of nearly $1.8 million in professionals' fees filed for AMCA counsel (consisting of bankruptcy counsel, counsel for regulatory matters and special counsel for a landlord-related matter). AMCA estimated another $300,000 of administrative-expense claims existed for nonprofessional claims accruing post-petition.

In sum, the costs and consequences of the data breach were quite severe. Most obviously, AMCA was forced to cease operations, as it was too damaged to seek an orderly chapter 11 restructuring or sale and ultimately too poor to afford an orderly liquidating plan. However, AMCA escaped the uncertainty of a chapter 7 proceeding — and used its time in chapter 11 effectively to reach resolution with a large number of state attorneys general — but only at a very significant personal cost to the principal. Other substantial consequences included the loss of employment for approximately 100 AMCA employees, the lack of any distribution to unsecured creditors, and the impact on the millions of people whose PII was improperly disclosed.

Conclusion

A data breach can be the equivalent of a knockout punch in some circumstances, thus making reorganization impossible. Furthermore, the costs and consequences of a breach can escalate quickly. Although no other situation will involve the exact facts as presented by AMCA, hopefully an understanding of the case will help business leaders (and their outside professionals) appreciate the value of risk-mitigation and investing in resiliency. abi

Reprinted with permission from the ABI Journal, Vol. XL, No. 3, March 2021.

12 *Id.* D.E. 339 (*see* Order Pursuant to Fed. R. Bankr. P. 9019(A) Approving Settlement and Authorizing Acceptance of Form of Agreed Final Judgment Between the Debtor and Participating State Attorneys General).
13 *Id.* D.E. 357 (Order Dismissing Chapter 11 Case and Granting Related Relief).