95th Annual National Conference of Bankruptcy Judges
October 6-9, 2021 Indianapolis, Indiana

CYBERSECURITY 2021: THE CAUTION FLAG REMAINS OUT

John G. Loughnane, Partner, Nutter McClennen & Fish LLP

CYBERSECURITY 2021:
THE CAUTION FLAG REMAINS OUT
Table of Contents

Threat Landscape

1. Discussion Topics

a) Business e-mail compromise (BEC)

b) Spoofing and phishing

c) Ransomware

d) Threat Actors (including insider threat)

2. Resources

Ethical Duties

1. Discussion Topics

a. Competence

b. Confidentiality

c. Communication

d. Incident Response

2. Resources

a. *2020 Cybersecurity,* AMERICAN BAR ASSOCIATION TECHREPORT 2020 (October 19, 2020). By John G. Loughnane (of Nutter, McClennen & Fish, LLP) 4

b. *Technology and Legal Ethics: A User's Manual (Part I)*, XXXIX ABI JOURNAL 2, 12, 49-51, February 2020. By Elizabeth B. Vandesteeg (of Levenfeld Pearlstein, LLC) 7

c. *Technology and Legal Ethics: A User's Manual (Part II),* XXXIX ABI JOURNAL 4, 24-25, 64, April 2020. By Elizabeth B. Vandesteeg (of Levenfeld Pearlstein, LLC) 10

d. ABA Model Rules of Professional Conduct available at https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/

   i. Model Rule 1.1: Competence

   ii. Model Rule 1.6: Confidentiality

   iii. Model Rule 1.4: Communication

e. ABA Standing Committee on Ethics and Professional Responsibility available at https://www.americanbar.org/groups/professional_responsibility/committees_commissions/ethicsandprofessionalresponsibility/

   i. Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack

   ii. Formal Opinion 477R: Securing Communication of Protected Client Information

Hot Topics

1. Discussion Topics

a. Virtual Practice

b. Incident Response Plan

c. Policies and Procedures

d. Tech Tips

2. *Resources*

a. *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition,* AMERICAN BAR ASSOCIATION. Edited by Jill Rhodes and Robert S. Litt available at https://www.americanbar.org/products/inv/book/309654847/

b. *Resources for Lawyers,* CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, available at https://www.cisa.gov/resources-lawyers

c. *Preparing for a Cyber Incident,* UNITED STATES SECRET SERVICE, available at https://www.secretservice.gov/sites/default/files/reports/2020-12/Preparing%20for%20a%20Cyber%20Incident%20-%20An%20Introductory%20Guide%20v%201.1.pdf

d. *Internet Crime Complaint Center (IC3),* FEDERAL BUREAU OF INVESTIGATION, available at https://www.ic3.gov/

e. *National Cybersecurity Alliance*, available at https://staysafeonline.org/

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 costsand 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 ulimately 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 chap- ter 7) was in the best interests of creditors — and only pos- sible 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 "FirstDay" 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), *avail- able 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).

October 19, 2020
TECHREPORT 2020

2020 Cybersecurity

John G. Loughnane

Share:

The results are in for this year's *Legal Technology Survey Report* conducted by the American Bar Association's Legal Technology Resource Center (LTRC). As in past years, the *2020 Survey* collected information from attorneys in private practice on a host of topics concerning the use of technology in the practice of law. Responses came from attorneys practicing in a wide range of settings: solos (26%); firms of 2-9 attorneys (30%); firms of 10-49 attorneys (17%); firms of 50-99 attorneys (5%); firms of 100-499 attorneys (10%), and firms of 500+ attorneys (12%).

Using the information collected, the LTRC prepared its *2020 Survey,* consisting of five volumes:

1. Technology Basics & Security
2. Law Office Technology
3. Marketing & Communication Technology
4. Online Research
5. Litigation Technology & E-Discovery

The *2020 Survey* includes a detailed analysis of the responses to the 262 questions, along with trend reports comparing results to prior years. The "Technology Basics & Security" responses were for 21 questions focused on security, covering technology policies, security tools, security breaches, viruses/spyware/malware, physical security measures, and backup.

This *TechReport* discusses how the *2020 Survey* results compare to prior years in the specific areas of incident awareness and incident response planning. First, however, it is appropriate to consider generally the ethical and legal issues at stake as well as the state of cybersecurity threats at the current time.

Ethical and Legal Considerations; Cybersecurity Threats

Last year's cybersecurity *TechReport* discussed fundamental ethical rules of competency, communication, and confidentiality which underscore the importance of cybersecurity to the profession. Those rules remain very much applicable and should be ingrained into daily practice. In addition, last year's *TechReport* noted ABA Standing Committee on Ethics and Professional Responsibility Formal Opinion 483 "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018), which provides that "the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach." The Opinion also states that "As a matter of preparation and best practices... lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach."

In addition to ethical obligations of the profession, lawyers and firms are bound as well, of course, to any applicable state and federal laws governing information security and data breach obligations—a point specifically recognized by Opinion 483. Legislative

attention in this area is rampant as evidenced by the Stop Hacks and Improve Electronic Data Security ("SHEILD") Act enacted by New York in 2019 and the California Consumer Privacy Act (CCPA) which became effective in January 2020.

Interestingly, the answers to the *2020 Survey* were collected between March and May 2020—a time when the impacts of COVID-19 were first suffered by many personally and professionally. During that time, numerous law firms shut down offices and moved all personnel to virtual, remote working environments. The ABA highlighted the heightened cybersecurity risks in March 2020 through a variety of means including a webinar on Remote Working in a Time of COVID-19: Cybersecurity Issues You Need to Know and discussion in articles such as "Experts Warn Lawyers of Cyber Risks to Remote Work."

Not surprisingly, the heightened concerns proved well justified. Reports of malicious activity intensified significantly affecting all corners of life including the legal profession. A prominent example includes the widely publicized ransomware attack on the law firm Grubman Shire Meiselas & Sacks, whose clients include numerous high-profile celebrities. As of this writing, reports indicate the firm has rebuffed demands for payment and faces the threat that confidential client data will be auctioned off in the summer of 2020.

Despite the ethical issues and pending challenges, the *2020 Survey* results reveal that the use of certain security tools remains at less than half of respondents. For example, 43% of respondents use file encryption, 39% use email encryption, 26% use whole/full disk encryption. Other security tools used by less than 50% of respondents are two-factor authentication (39%), intrusion prevention (29%), intrusion detection (29%), remote device management and wiping (28%), device recovery (27%), web filtering (26%), employee monitoring (23%), and biometric login (12%).

In contrast to the continuing slow adoption of security tools, this year's results do indicate an increasing number of firms committing to cyber liability insurance policies—36% percent of respondents, compared to 33% in 2019, 34% percent in 2018, and 26% in 2017. Firms ranging in size from 10-49 attorneys are most likely to have cyber liability insurance (40%), followed closely by firms of 100+ attorneys (38%). One notable trend is the increase in the number of smaller firms with such coverage, with firms of 2-9 attorneys (36%) and solo attorneys (33%) up respectively from 27% and 19% since 2017.

With the ethical imperative for security very clear, the threat environment pronounced, and the use of security tools not widely adopted, one apparent trend revealed by the *2020 Survey* is an effort by the profession to cover risk through insurance. Certainly, firms are wise to have policies in place, but a policy is only one component of an appropriate comprehensive, risk-based security program and itself offers no protection from attack nor any guarantee of actual coverage. The responsibilities and challenges could not be any clearer—and the profession needs more attention on the issues beyond merely increased insurance purchases.

Incident Awareness

The *2020 Survey* results show that the number of firms experiencing a security breach (such as a lost/stolen computer or smartphone, hacker, break-in, website exploit) increased over the prior year; 29% of respondents compared to 26% in 2019.

The number of respondents continuing to report that they do not know whether their firm has ever experienced a security breach remains high at21%, compared to 19% for the prior year. As in the past, the larger the firm, the greater percentage of those unaware of whether their firms have ever experienced a breach (1% of solo respondents; 9% of firms of 2-9 attorneys; 28% of firms of 10-49 attorneys; 62% of firms of 100+ attorneys).

Reported consequences of security incidents revealed some interesting trends. For example, just 32% of respondents indicated the need to incur consulting fees for repair (down from 37% in 2019 and 40% in 2018). Similarly, a downward trend appears in the number of respondents reporting downtime/loss of billable hours at 34% (down from 35% in 2019 and 41% in 2018), as well as the destruction or loss of files (11% down from 15% in 2019).

In contrast, upward trends were reported in connection with the expense for replacing hardware or software (28% compared with 20% in 2019), notifying law enforcement of breach (14% compared with 9% in 2019), notifying clients of the breach (11% compared

with 9% in 2019), unauthorized access to non-client sensitive data (7% up from 4% in 2019), and unauthorized access to sensitive client data (8% compared to 3% in 2019).

On the topic of viruses, spyware, and malware, results in two areas match 2019: 36% of respondents have had systems infected and 26% again were not aware whether any such infection has ever occurred. The size of a firm continues to impact the awareness level of respondents: only 4% of solo respondents report they "don't know" (down from 7% in 2019), while the percentage is 15% of respondents in firms of 2-9 attorneys (same as 2019), 39% of attorneys in firms of 10-49 attorneys (up from 30% in 2019), and 57% of attorneys in firms of 100+ attorneys (down slightly from 58% in 2019).

When asked what business losses/breaches resulted from a virus, spyware, or malware attack, 70% of respondents reported that they believed no significant business disruption or loss resulted. This response continues the upward trajectory over the past few years (60% in 2019, 62% in 2018, and 61% in 2017). The trend mimics the response given by respondents who have experienced a security breach—67% reported their belief that no significant business disruption or loss occurred (up from 65% in both 2019 and 2018, and 62% in 2017). In reviewing these results, it is only natural to wonder whether the seemingly positive trends reflect a troubling false sense of comfort in the short term amid the prospect of potentially longer-term harm.

Consequences identified by respondents resulting from a virus, spyware, or malware infection include costs incurred for consulting fees for repair (39%), downtime/loss of billable hours (35%), temporary loss of network access (23%), temporary loss of web site access (10%), and replacement of hardware/software (17%). All these types of consequences are readily apparent while other adverse consequences may go unnoticed.

Incident Response Plans

The *2020 Survey* response reveals continued improvement on the topic of developing incident response plans, with 34% of respondents indicating their firms maintained such a plan, up from 31% in 2019 and 25% in 2018. The likelihood of a firm having one remains a function of firm size. Thus, 77% of respondents from firms of 100+ attorneys reported that their firms have an incident response plan (up from 65% in 2019), 38% of respondents from firms of 10-49 (up from 35% in 2019), 23% of respondents from firms of 2-9 (up from 19% in 2019), and 14% of solo respondents (up from 11%).

Incident response plans remain a critical element of any information security program. The above results clearly show an expanded adoption of incident response plans. Yet, there remains room for improvement. The LTRC has been conducting some form of the *Legal Technology Survey Report* for nearly three decades. How long will it take before every firm has in place a basic incident response plan? The progress has been trending in the right direction, but the pace is glacial given the ethical and legal issues discussed earlier along with the heightened threat environment. Opinion 483 should be a starting point for any firm tackling this issue.

Conclusion

The *2020 Survey* largely reflects incremental progress in areas fundamental to adequate security, in an age which cries out for a much more robust response by the profession to the challenges at hand. The balance of the year is an excellent opportunity for firms to anticipate the questions that will be asked in the *2021 Survey* next March and take appropriate action now.

Meanwhile, some impetus for improving the pace of change in this area has emerged: the approval in June 2020 by the New York State Bar Association of a report by its Committee on Technology and the Legal Profession recommending that one credit of mandatory continuing legal education in ethics be devoted to cybersecurity. If approved, New York would join two other states (Florida and North Carolina) requiring a technology component as part of continuing legal education programs, as tracked by Bob Ambrogi. Although this development is notable, professionals need not wait for the profession to mandate education—all the information needed to act is available now. And just as an insurance policy will not prevent a hack, neither will a course; ultimately, professionals in firms of all sizes need to synthesize good cybersecurity practices into the everyday practice of law.

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

Cyber-U

By ElizaBEth B. VandEstEEg

Technology and Legal Ethics: A User's Manual (Part I)

Coordinating Editor Elizabeth B. Vandesteeg
Sugar Felsenthal Grais & Helsinger, LLP Chicago

Lisa Vandesteeg is chair of the Litigation and Dispute Resolution Group of Sugar Felsenthal Grais & Helsinger LLP in Chicago. Her practice includes bankruptcy, commercial litigation, business disputes and privacy and data-security issues. She is a Certified Information Privacy Professional for the U.S. Private Sector, as qualified by the International Association of Privacy Professionals. A 2017 ABI "40 Under 40" honoree, she serves as an associate editor for the ABI Journal.

Once upon a time, certain attorneys embraced the view that being a Luddite[1] was a point of pride; they had practiced in paper for decades, and new-fangled technology was unnecessary to provide top-notch service to their clients. This worldview has ever-decreasing adherents, as technology has reached into nearly every facet of the practice of law. Not only is facility with technology a practical business requirement to adequately serve clients, it is now also an ethical requirement imposed upon attorneys in most states. Standard rules of professional conduct mandate that attorneys both take reasonable steps to keep the client data that they hold secure and provide notice to clients should there be an unauthorized disclosure of such data.

For bankruptcy attorneys, the implications of these standards are particularly far-reaching. While commercial litigators and their transactional counterparts might be privy to confidential data, it is likely that such information will be discrete and related solely to the dispute or deal at issue. There will be only a few parties involved, and the process will not require public disclosures beyond limited public filings.

On the other hand, bankruptcy is a process that requires comprehensive disclosures and involves numerous parties. Bankruptcy attorneys, particularly those representing corporate debtors, might find themselves responsible for an entire company's data, including all financial, proprietary and employee information. They must understand the types of potentially sensitive information in their possession and the proper ways to safeguard it from unauthorized access or disclosure.

This article is the first in a two-part series discussing the fundamentals of the intersection of cybersecurity and ethics for bankruptcy attorneys. This article discusses the key ethical rules in the realm of technology and data security. The second article, which will appear in a later issue, will provide guidance as to the best practices with respect to securing and transferring client data as part of information-security programs for law firms, as well as the necessary steps that law firms must take to notify clients in the event of a data breach and loss of client information.

Technological Competence: The Cornerstone of Cyber Ethics

Any attorney's first and most important ethical duty to clients is to provide competent legal representation. Model Rule 1.1 of the American Bar Association's (ABA) Model Rules of Professional Conduct[2] requires that such "competent representation" to a client include the requisite legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[3]

An attorney's ability to provide that competent representation includes a requirement of technological facility. Specifically, Comment 8 to Model Rule 1.1 requires an attorney to keep abreast of "the benefits and risks associated with relevant technology."[4] With this addition, the Model Rule's definition of "competency" now mandates that attorneys maintain both a substantive knowledge of law *and* proficient skills with the ever-evolving technology available to attorneys and clients.

1 A "Luddite" is defined as someone "who is opposed to especially technological change." *Merriam-Webster Dictionary*, *available at* merriam-webster.com/dictionary/Luddite (last visited Jan. 7, 2020).

2 The ABA Model Rules of Professional Conduct were adopted by the ABA House of Delegates in 1983 and serve as models for the ethics rules of most U.S. jurisdictions. Some variation has been adopted by all 50 states.

3 Model Rules of Prof'l Conduct R. 1.1 (2019).

4 Model Rules of Prof'l Conduct R. 1.1, cmt. 8 (2019) (adopted in 2012).

In the seven years since the ABA adopted Comment 8 to Model Rule 1.1, 38 states have included similar requirements in their ethical rules.[5] For attorneys, achieving and maintaining a certain level of technological proficiency is simply no longer optional.[6]

What to Do?

Technology invades nearly every province of legal practice — from the use of timekeeping and billing software to the redaction required of e-filers to e-discovery, and from vetting vendors for security compliance to training staff and attorneys on recognizing security risks. The complex relationship between new technological opportunities and the accompanying risks can create a confusing landscape for attorneys.

For example, the use of third-party service providers, such as cloud-based document-management and storage companies, might benefit an attorney in the form of increased efficiency in moving away from paper records. However, that attorney must monitor how those service providers secure and store client data. The widespread availability of public wireless networks also provides attorneys with the chance to check email and perform work remotely from nearly any location, but such networks also bring heightened risk of exposing client data to bad actors who monitor and intercept internet traffic on those networks.

How, then, do attorneys comply with this requirement for technological competence? "Competence" in technology cannot be satisfied by merely hiring qualified IT personnel and considering the matter solved. The Model Rules make it clear that attorneys must educate themselves on both the risks and benefits of technology, either through self-study (*e.g.*, by attending continuing legal education seminars, such as those offered at ABI conferences), associating with knowledgeable individuals in their law practice, or otherwise receiving training on relevant technology.[7]

Attorneys must know enough about the new technology they use to perform legal services to ensure that they are compliant with their professional responsibilities to keep client information confidential and secure. An attorney using new technology without learning how to operate it safely is running afoul of the fundamental ethical obligations.

Confidentiality: Lock It Up

While technology may have changed the means by which attorneys maintain and transmit sensitive information, the duty of confidentiality remains unchanged. Model Rule 1.6 prohibits an attorney from revealing "information relating to the representation of a client" unless such client gives informed consent, or the disclosure is "impliedly authorized" or otherwise permitted.

Attorneys are ethically required to make "reasonable efforts" to prevent inadvertent or unauthorized disclosure of — or unauthorized access to — information relating to the representation of a client (or former client).[8] Attorneys can take some comfort in knowing that the Model Rules provide that unauthorized access or inadvertent disclosure of client information "does not constitute a violation of paragraph (c) [of Model Rule 1.6] if the lawyer has made reasonable efforts to prevent the access or disclosure."[9]

> **Attorneys must train themselves, their employees and their vendors in the use of reasonable, situation-specific safeguards for client data and other sensitive information.**

In typical lawyerly fashion, the "reasonable efforts" standard is a fuzzy one, and the determination of whether efforts are indeed reasonable is a fact-specific inquiry. Relevant factors include the sensitivity of the information, the risk of disclosure without additional precautions, the cost of extra measures, the difficulty of adding safeguards, and whether more safeguards adversely affect the lawyer's ability to represent the client.[10]

The onus is also on an attorney to analyze and determine any appropriate safeguards regarding the transmission of confidential information. The Model Rules specify that this does not necessarily require the use of special security measures (such as encrypting every email), but prompt lawyers to consider whether special security measures are warranted with respect to particularly sensitive information or material protected by law or confidentiality agreements.[11]

What to Do?

The "reasonable efforts" standard requires an informed and delicate balancing act. Attorneys must implement strong data-security practices in order to safeguard client data and comply with ethical responsibilities. However, at the same time, attorneys must take into account both the actual cost of additional security measures (technologi- cal or otherwise), and also the potential adverse impact of such security on the lawyer's ability to practice law. For example, while requiring encryption of every document ina firm's database might make the data extremely secure, it would also create a practical inability for attorneys to effi- ciently perform work.

This standard requires attorneys to be well-versed enough in technological matters to appropriately assess what security measures are sufficient and when. For exam- ple, "reasonable efforts" for an attorney dealing with an individual client's personal or financial data may involve encrypting any email providing that information to another recipient or arranging for an alternative means of secure

5 At the time of this article, 11 states have yet to enact versions of Comment 8 in their rules of professional responsibility or otherwise recognize the technological competence duty: Alabama, Alaska, Georgia, Hawaii, Maine, Maryland, Mississippi, Nevada, New Jersey, Oregon and South Dakota. While one of the remaining states, California, has not formally adopted the change to its rules of professional conduct, it has issued an ethics opinion expressly acknowledging the technological competence duty in the context of e-discovery in litigation. State Bar of Calif. Standing Comm. Prof'l Responsibility and Conduct Formal Op. No. 2015-109 (2015).

6 At least two states, Florida and North Carolina, now mandate not only technological competence, but also technology training as part of their continuing legal education programs.

7 Model Rules of Prof'l Conduct R. 1.1, cmts. 1, 6, 8 (2019). *See, e.g., James v. Nat'l Fin. LLC*, No. 8931-VCL, 2014 WL 6845560 (Del. Ch. Dec. 5, 2014) (discussing competence as requirement of Pennsylvania and Delaware rules of professional conduct in the context of e-discovery violations).

8 Model Rules of Prof'l Conduct R.1.6(c) and cmt. 20 (2019) (adopted in 2012).

9 Model Rules of Prof'l Conduct R. 1.6, cmt. 18 (2019).

10 *Id. See, e.g.*, State Bar of Ariz. Ethics Op. 09-04 (2009) (discussing standards for electronic access to client files).

11 Model Rules of Prof'l Conduct R. 1.6, cmt. 19 (2019).

transmission. For example, an attorney representing a corporation seeking to sell its assets pursuant to § 363 of the Bankruptcy Code should perform due diligence on the cloud-based document-hosting service that might be used as the data room to confirm that it has sufficient security safeguards in place. Attorneys must also be aware of and avoid common and well-known data security risks, such as the use of unsecured wireless networks in coffee shops and airports, and instead use a secured wireless network to communicate with clients.

Supervisory Responsibilities

Attorneys are required to not only be competent in their own legal practice but also be responsible for the actions taken by those under their supervision.

Junior Attorneys

Partners and other supervisory attorneys are required to "make reasonable efforts" to ensure that the firm has in effect measures "giving reasonable assurance" that all lawyers in the firm conform to the ethical rules. A supervising attorney must also make "reasonable efforts" to ensure that junior lawyers adhere to the ethical rules.[12]

When considering those responsibilities in the context of technology and data security, senior attorneys must instruct junior attorneys on the responsibility to safeguard client data. Supervisory attorneys must provide training (ideally as part of and in compliance with a holistic information-security program) on critical security issues, including using care when emailing recipients outside the firm; avoiding the use of public unsecured wireless networks; and properly securing devices containing client data such as mobile phones, tablets and laptops. Partners cannot turn a blind eye when they see junior lawyers failing to take such precautions, or they risk ethical violations themselves.

Nonlawyer Employees and Vendors

Similarly, lawyers are responsible for overseeing nonlawyers employed or retained by, or associated with, a lawyer. This rule contemplates the oversight responsibilities triggered by an attorney's use of both nonlawyer employees within a firm and service providers outside the firm, and requires an attorney to take "reasonable efforts" (there is that fuzzy standard again!) to ensure that services are pro- vided in a manner that is compatible with the lawyer's professional obligations.[13]

Law firms regularly employ nonlawyers, including paralegals, secretaries or law clerks. A lawyer must give such assistants "appropriate instruction and supervision" concerning the ethical aspects of their employment, "particularly regarding the obligation not to disclose information relating to the representation of a client."[14]

Attorneys also frequently make use of external vendors in legal practice, such as investigators, expert witnesses, e-discovery vendors and cloud-based services for hosting firm and client data. For bankruptcy practitioners, this mightalso include third parties such as claims and noticing agents.

What to Do?

What do these supervisory responsibilities require on a practical level? Read in tandem with the competence required of Model Rule 1.1 and the need to safeguard client confidences in Model Rule 1.6, these supervisory responsibilities require attorneys to know enough about technology and data security to appropriately hire and supervise junior attorneys, nonlawyers and service providers.

An attorney may not simply hire any vendor they hear about without first investigating that vendor's particular data-security practices and confirming that the vendor stores and transmits any data it handles in a manner that is compatible with that attorney's professional obligations. "Reasonable efforts" to ensure that an external vendor is performing its work in a manner compatible with the lawyer's professional obligations should include consideration of such factors as "the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."[15]

Similarly, there is no way for an attorney to avoid ethical responsibilities by blaming a breach on an assistant who may have clicked on a bad email link or responded to a fraudulent request for a wire transfer. Attorneys, particularly supervisory attorneys such as partners, should implement an information-security program to ensure that proper supervision and standards are in place in order to comply with ethical responsibilities. An attorney should also provide training to staff members in areas such as email security awareness, proper procedures for sending and receiving wire transfers, procedures for storing and destroying client documents and data, and protocols for sending client data outside the firm.

Conclusion

Technological competence and appropriate data-security measures are no longer a problem that can be outsourced to IT. Attorneys must train themselves, their employees and their vendors in the use of reasonable, situation-specific safeguards for client data and other sensitive information. This is not only a prudent business move, but it is also required by ethical rules in most states. With proper training and oversight, attorneys can comply with these ethical rules and ensure the security of client data. **abi**

Reprinted with permission from the ABI Journal, Vol. XXXIX, No. 2, February 2020.

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.

12 Model Rules of Prof'l Conduct R. 5.1 (2019).
13 Model Rules of Prof'l Conduct R. 5.3 (2019).
14 Model Rules of Prof'l Conduct R. 5.3, cmt. 2 (2019).

15 Model Rules of Prof'l Conduct R. 5.3, cmt. 3 (2019). *See, e.g.*, Ill. State Bar Assoc. Advisory Op. No. 16-06 (2016) (discussing "reasonable efforts" to employ when selecting and hiring cloud computing vendor).

66 Canal Center Plaza, Suite 600 • Alexandria, VA 22314 • (703) 739-0800 • Fax (703) 739-1060 • www.abi.org

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

Cyber-U

By ElizaBEth B. VandEstEEg

Technology and Legal Ethics: A User's Manual (Part II)

Coordinating Editor Elizabeth B. Vandesteeg
Sugar Felsenthal Grais & Helsinger LLP
Chicago

Lisa Vandesteeg is chair of the Litigation and Dispute Resolution Group at Sugar Felsenthal Grais & Helsinger LLP in Chicago. Her practice includes bankruptcy, commercial litigation, business disputes and privacy and data security issues. Ms. Vandesteeg is a Certified Information Privacy Professional for the U.S. Private Sector, as qualified by the International Association of Privacy Professionals. A 2017 ABI "40 Under 40" honoree, she serves as an associate editor for the ABI Journal.

As was discussed in Part I,[1] use of technology has become a vital and inescapable component of the practice of law. Society's now-ubiquitous reliance on technology has required the legal industry to augment the ethical standards that attorneys must uphold in order to maintain fundamental protections for their clients and their clients' information. These ethical standards are applicable to all attorneys equally, but they are particularly relevant for bankruptcy attorneys, who are custodians of a host of personally identifiable information (PII)[2] and other sensitive and confidential information.

Part II of this article will focus on the specific ethical obligations and practical standards set forth in two recent American Bar Association (ABA) ethics opinions governing the storage and transmittal of client data, as well as the necessary steps that lawyers and firms must take to protect against, and notify clients of, any unauthorized access to client information.

Securing Communication of Protected Client Information

On May 11, 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "Securing Communication of Protected Client Information." Acknowledging that law firms are high-quality targets of hackers, the purpose of Formal Opinion 477R was to address "how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world."[3]

The ABA's conclusion is that "[a] lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access." How, then, should one determine what steps are "reasonable" to prevent unauthorized access to client information? Formal Opinion 477R expressly states that it is "beyond the scope" of the opinion to expressly dictate what may constitute "reasonable steps" to protect client data, but it provides the following "considerations as guidance":

1. *Understand the nature of the threat:* A lawyer must consider the sensitivity of the client's information and whether the information is at a higher risk for cyberattack (*e.g.*, trade secret or financial information); higher-risk scenarios require greater efforts to protect.[4]
2. *Understand how client confidential information is transmitted and where it is stored:* A lawyer must understand the law firm's technological landscape in terms of how electronic communications are created, where client data is stored, and how and by whom the data can be accessed.[5]
3. *Understand and use reasonable electronic security measures:* A lawyer should understand the various options that exist to protect electronic information and implement appropriate measures to protect client data and communications. This could include the use of secure internet access methods (secure Wi-Fi or virtual private network); complex passwords; firewalls; anti-malware/antivirus software; regular security patches and updates; encryption; and multifactor authentication.[6]

1 Elizabeth B. Vandesteeg, "Technology and Legal Ethics: A User's Manual (Part I)," XXXVIX *ABI Journal* 2, 12, 49-51, February 2020, *available at* abi.org/abi-journal (unless otherwise specified, all links in this article were last visited on Feb. 26, 2020).
2 PII is defined as "[a]ny information about an individual, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linkable to an individual, such as medical, educational, financial, and employment information." "Personally Identifiable Information," IAPP Resource Center, *available at* iapp.org/resources/article/personally-identifiable-information.
3 ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R, at 2 (2017).
4 *Id.* at 6.
5 *Id.*
6 *Id.* at 6-7.

66 Canal Center Plaza, Suite 600 • Alexandria, VA 22314 • (703) 739-0800 • Fax (703) 739-1060 • www.abi.org

4. *Determine how electronic communications about clients' matters should be protected:* A lawyer and client should discuss what levels of security will be required for electronic communications, recognizing that communications might be at varying levels of sensitivity and could require different degrees of protection.[7]

5. *Label clients' confidential information:* A lawyer should mark client communications as "privileged and confidential" in order to put any unintended recipi- ent on notice of the intent for the communication to remain confidential.[8]

6. *Train lawyers and nonlawyer assistants in technology and information security:* Applying ABA Model Rules 5.1 and 5.3, lawyers must establish policies regarding, and train employees on the use of, secure methods of communication with clients and reasonable measures for the storage of and access to client data and communications.[9]

7. *Conduct due diligence on vendors providing communication technology:* A lawyer must take reasonable steps to analyze potential vendors who will be involved in the transmittal or storage of client data or communications. Lawyers should consider reference checks and vendor credentials; vendor security policies and hiring practices; use of confidentiality agreements; and availability of legal fora in the event of violations of the vendor agreement.[10]

From the perspective of a cybersecurity attorney, these "considerations" are the framework of a basic information security program. The creation and implementation of a thoughtful and deliberate information security program, as evidenced by and set forth in a written information secu- rity policy evidencing its terms, is a best practice that everylaw firm should follow. Simply put, an information security policy is a company's documented statement of rules and guidelines that need to be followed with respect to the security of company data. For a law firm, an information security policy should expressly apply to client data, and it should detail the administrative, physical and technical safeguards in place to provide reasonable protection of client information.

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Data loss and hacking are now commonly discussed in terms of "when" and not "if." Even an attorney who has taken reasonable steps to protect client data and communications may well nonetheless be the target of a cybersecurity incident or data breach involving client information. How should an attorney ethically handle and respond to such an event?

On Oct. 17, 2018, the ABA Ethics Committee issued Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack." Formal Opinion 483 "picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information.[11] It sets forth both obligations related to the detection of and response to a cybersecurity incident, as well as specific notice requirements to clients.

For purposes of Formal Opinion 483, a data breach occurs when "material client confidential information is misappropriated, destroyed, or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired."[12] But not every data breach will result in an ethical violation — only those where "a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach."[13]

Reasonable Efforts to Prevent a Data Breach

In the first instance, lawyers have an obligation to monitor for data breaches.[14] They must monitor firm technology and resources connected to the internet, as well as external data sources and external vendors who might access or provide services involving client data.

Lawyers and law firms should also proactively develop a detailed incident response plan (IRP) before a breach occurs, so that appropriate and coordinated steps might be taken immediately thereafter.[15] While every lawyer's IRP should be tailored to fit their office's or firm's specific practice, the fundamental goal of any IRP is to appropriately handle an incident through (1) preparation; (2) detection and analysis; (3) containment, eradication and recovery; and (4) post-incident activity.[16]

As part of the preparation phase, it is important to draft the IRP as a simple standalone document. It should designate and provide contact information for team members and their backups (a "breach response team"), together with the specific roles that each member will play in the event of a security incident, and at every stage of the incident.[17] Best practices then encourage the breach response team to engage in "tabletop exercises" in order to test and practice the IRP procedures before a security incident happens.

After taking prompt action to contain and eradicate the breach, a lawyer is ethically obligated to "make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients."[18] The extent of such efforts, whether through restoration of existing systems or through implementation of new technology, will depend on the specific circumstances of the breach. Unless the lawyer or firm is trained in this area, it is best to outsource this process to trained experts to ensure complete recovery and prevent further breaches.

Attorneys must then make reasonable efforts to determine what actually occurred during the data breach. Ethical standards governing post-breach investigations require that the lawyer have enough information to both confirm that the

7 *Id.* at 7-8.
8 *Id.* at 8.
9 *Id.* at 9.
10 *Id.* at 9-10.
11 ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 483, at 2 (2018) ("ABA Formal Op. 483").
12 *Id.* at 4. It is important to note that this definition is applicable only to determining whether attorneys have ethical obligations arising out of the applicable ABA Model Rules and Formal Opinions. This defini-tion is not the one that might be applicable should a loss of client information also trigger notification requirements under various state or federal data-breach-response laws.
13 ABA Formal Op. 483 at 5-6.
14 *Id.* at 4-6.
15 *Id.* at 6 (citing Jill D. Rhodes & Robert S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals* (2d ed. 2018)).
16 Nat'l Inst. of Standards and Tech., *Computer Security Incident Handling Guide*, at 21-45 (2012), *available at* nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
17 ABA Formal Op. 483 at 6-7 (citing Steven M. Puiszis, "Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning," *The Prof'l Lawyer*, Vol. 24, No. 3 (November 2017)).
18 *Id.* at 7.

breach has in fact been contained and evaluate the extent, if any, to which client data was accessed or lost.[19] In addition, the post-breach investigation should be extensive enough to determine how the breach occurred in order to patch any and all vulnerable access points.

Obligations to Provide Notice of Data Breach

The Model Rules of Professional Conduct require that a lawyer must "keep the client reasonably informed about the status of a matter" and "shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."[20] Formal Opinion 483 interprets these rules to impose an ethical obligation on a lawyer to communicate with current clients about a data breach.[21]

Current clients are entitled to notification when a data breach occurs that involves, or likely involves, material client confidential information.[22] Upon disclosing a breach to a client, a lawyer must provide enough information for the client to make an informed decision about what to do next, if anything, with respect to the present representation. This means that a lawyer must disclose to the client not only the occurrence of, but also the extent of, the unauthorized access to or disclosure of the confidential client information. Lawyers should be prepared to advise the client regarding the breach response plan, the efforts being taken to recover the client information, and any additional measures being implemented to increase data security and prevent future breaches.[23]

Finally, and apart from ethical obligations, if a data breach involves unauthorized access to PII, whether of clients or others, a lawyer must examine potential notification obligations under various state and federal laws. All 50 states have adopted breach-notification laws, with differing definitions of "protected information" and "breach," and differing standards for scope and requirements of notice.[24]

Conclusion

Lawyers are individuals governed by ethical obligations with respect to the confidential information entrusted to them by their clients. However, law firms are businesses, with the goal of making a profit for the partners or shareholders, and the interests of individual lawyers and the businesses they work for can sometimes conflict.

Fortunately, there is great overlap between best business practices and legal ethical obligations with respect to data security. To check both boxes, lawyers and their firms should be very deliberate in creating and implementing an information security program that appropriately protectsa firm's most valuable asset: its clients' information and communications. This can only be done if lawyers take the necessary time to familiarize themselves with the technologies they use, implement set standards for how client data will be stored and accessed (through the use of a written information security policy), install preventive measuresto protect against breaches, and know what to do if/whena breach occurs (through the use of an incident response plan). Failing to follow this protocol risks inviting other- wise-avoidable liability that can threaten a lawyer's practiceand reputation. **abi**

Reprinted with permission from the ABI Journal, Vol. XXXIX, No. 4, April 2020.

19 *Id.* at 7-8.
20 Model Rules of Prof'l Conduct R. 1.4(a)(3) and 1.4(b) (2019).
21 ABA Formal Op. 483 at 10-12.
22 As a matter of legal ethics, this notification obligation does not extent to former clients "in the absence of a black-letter provision requiring such notice." Rather, lawyers are encouraged either to reach a specific agreement with the client about how to handle electronic information post-representation, or to adopt a general document-retention policy to reduce overall the amount of information retained of former clients. ABA Formal Op. 483 at 13.
23 ABA Formal Op. 483 at 14-15.
24 *Id.* at 15 (citing to Nat'l Conference of State Legislatures, Security Breach Notification Laws (Sept. 29, 2018), *available at* ncsl.org/research/telecommunications-and-information-technology/security-breach-

notification-laws.aspx).

66 Canal Center Plaza, Suite 600 • Alexandria, VA 22314 • (703) 739-0800 • Fax (703) 739-1060 • www.abi.org