February 5, 2018

# Cybersecurity for Law Firms: Recent Developments

Barry R. Temkin
Atea Martin

New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 24
MONDAY, FEBRUARY 5, 2018

Outside Counsel

Expert Analysis

# Cybersecurity for Law Firms: Recent Developments

BY BARRY R. TEMKIN AND ATEA MARTIN

While abundant publicity has accompanied spectacular data breaches at Equifax and Yahoo, less attention has been paid to cybersecurity at law firms. This, however, is changing, as cybersecurity events, including hacking, are on the rise at law firms. A major professional liability insurer estimates that as many as 80 percent of the largest law firms in the U.S. have experienced data breaches recently. "Safe and Secure: Cyber Security Practices for Law Firms," *CNA Professional Counsel*. Moreover, information stored in the cloud or transmitted via unsecured servers may be vulnerable to unauthorized intrusions.

Recent law firm data breaches have included the outside hacking by Chinese nationals into the computers of the mergers and acquisitions groups at two major law firms, resulting in significant insider trading and an enforcement case by the U.S. Securities & Exchange Commission against the overseas nationals (but not the law firms). In addition, former clients of a Chicago law firm filed a federal class action against the law firm alleging that they were injured because of the firm's failure to maintain data security—even though there were no allegations of actual intrusions.

Barry R. Temkin and Atea Martin

These alarming developments have been accompanied by an increase in government scrutiny of regulated industries and the lawyers who serve them. In addition, the organized bar has issued recent ethics opinions which may presage a trend toward enhanced vigilance by lawyers on encryption and other cybersecurity requirements. This article will analyze recent developments in lawyer cybersecurity and explain the nascent but growing trend toward stepped-up scrutiny of law firm data protection, including by state ethics regulators and the organized bar.

## Recent Law Firm Data Breaches

The data breach of Panamanian law firm Mossack Fonseca in 2016 embarrassed the firm's roster of affluent and politically powerful clients. See Frances Ivens, "Panama Papers Put Spotlight on Law Firm Data Security," *American Lawyer* (April 4, 2016). This infamous hack resulted in unwelcome publicity to the firm and its international clients, whom the Panamanian lawyers had apparently helped set up off-shore entities to evade their respective countries' income taxes on eye-popping wealth.

BARRY TEMKIN *is a partner at Mound Cotton Wollan & Greengrass, an adjunct professor at Fordham University School of Law and a member of the NYCLA Committee on Professional Ethics.* ATEA MARTIN *is Vice President, Life Agent and Broker Dealer Claims for Berkshire Hathaway Specialty Insurance, and a graduate of Brooklyn Law School.*

In 2016, the *Wall Street Journal* reported that two major U.S. law firms had been hacked by outsiders running an insider trading scheme seeking to benefit from non-public confidential information about potential mergers and acquisitions by the firms' clients. *Wall Street Journal* (March 29, 2016); *Bloomberg BNA* (March 30, 2016). The U.S. Securities & Exchange Commission subsequently filed an enforcement action against three Chinese nationals charged with insider trading based on hacked non-public information stolen from two New York based law firms. U.S. Securities & Exchange Commission, Litigation Release 23711/Dec. 27, 2016, *U.S. Securities & Exchange Commission v. Hong*. According to the SEC complaint, the Chinese hackers targeted the mergers and acquisitions departments of the firms, where they installed malware on the firm's networks, compromised accounts that enabled access to all email accounts at the firm and accessed dozens of gigabytes of emails from remote Internet locations.

A professional liability claim against a law firm for cybersecurity lapses was filed in 2016 against Chicago law firm Johnson & Bell, alleging that the firm committed malpractice by failing to maintain adequate standards of cybersecurity. Al Faikali, "Law Firm Data Security: The First Class Action," *Data Security Law Journal* (Dec. 12, 2016). The class action alleges that the firm, which portrays itself as an expert in advising clients about cybersecurity, was itself negligent in protecting its own clients' data security, by its failure to properly encrypt an online attorney time tracking system and the use of a virtual private network. Andrew Strickler, "Law Firm Hacking to Breed New Kind of Malpractice Suit," *Insurance Law 360* (Dec. 12, 2016). According to the federal complaint, "Johnson & Bell has injured its clients by charging and collecting market-rate attorney's fees without providing industry standard protection for client confidentiality." Id.

Aside from the fact that this is apparently the first class action against a law firm alleging cyber-insecurity, the Johnson & Bell suit is noteworthy in that the law firm was not hacked and there were no actual known data breaches. Rather, the purported class representatives alleged that they were damaged by the *risk* that their confidential information might be compromised at some point in the future. After denial of the law firm's motion to dismiss, the court directed the parties to participate in confidential arbitration, thereby reducing the likelihood that there will be additional reports on the case in the short term.

## New DFS Cybersecurity Regulations

Lawyers should also take note of new cybersecurity regulations promulgated by the New York Department of Financial Services, which regulates the insurance industry. These new cybersecurity rules, which apply to all entities under DFS jurisdiction, including insurance companies, insurance agents and banks, require encryption of all non-public information held or transmitted by the covered entity, and require each regulated company to appoint a chief information security officer (CISO), who must report directly to the board of directors and issue an annual report, setting forth an assessment of the company's cybersecurity compliance and any identifiable risks for potential breaches. Regulated entities must also implement dual factor authentication on their computer systems.

Of particular interest to law firms which represent financial institutions or are retained by insurance companies is §500.11 of the new DFS regulations, which requires each covered entity to "implement written policies and procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by third-parties doing business with the covered entity." 23 NYCRR §500.11. Thus, covered entities, including insurance companies, which provide access to personal identifying information to third-party vendors must certify not only that their own information systems are adequate, but also that the information security systems of vendors with whom they do business are also secure and protected. In other words, vendors who do business with regulated financial service companies will soon be expected to comply with the cybersecurity standards of their represented clients.

## The Organized Bar And Cybersecurity

The organized bar is now starting to look carefully at lawyers' ethical and professional liability respon-

sibilities to ensure the security of client data. Lawyers' duties of competence are embodied in New York Rule of Professional Conduct 1.1, which provides that: "A lawyer shall provide competent representation to a client." The New York State Bar Association Commentary to the Rules of Professional Conduct provides that: "To maintain the requisite knowledge and skill, a lawyer should … keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information … ." New York RPC 1.1, comment [8].

The New York Rules of Professional Conduct require lawyers to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. In March 2017, the New York County Lawyers Association issued NYCLA Ethics Opinion 749, which provides that lawyers are required by the RPC to keep up with technological developments, "cannot knowingly reveal client confidential information, and must exercise reasonable care to ensure that the lawyers, employees, associates and others whose services are utilized by the lawyer not disclose or use client confidential information." NYCLA Ethics Opinion 749 at 4. Significantly, the NYCLA ethics opinion recognizes a duty on the part of lawyers to prevent unauthorized data breaches:

> The risks associated with transmission of client confidential information electronically include disclosure through hacking or technological inadvertence. A lawyer's duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client information through hacking or errors in technology where the practice requires the use of technology to competently represent the client. Id.

These developments are forcing law firms to be cognizant of the very real and significant risks they face in the 21st Century, and to acquire the technology sufficient to keep abreast with their clients' cybersecurity needs.

In the same vein, in May 2017, the American Bar Association Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "Securing Communication of Protected Client Information." In its opinion, the ABA adopted "a fact-specific approach to business security obligations that requires a process to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments." ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 477R, May 22, 2017, at 4 (quoting from ABA Cybersecurity Handbook)

The ABA opined that the decision whether to use encrypted e-mail is fact-specific, and that lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, based upon a number of enumerated factors, including the sensitivity of the electronically-communicated information, the risk of cyber-intrusion and the needs of the client. Id at 7-8. Thus the organized bar is warning lawyers of their ethical obligation to maintain cybersecurity.

## Conclusion

As we have seen, law firm data breaches are on the rise, running the gamut from an unencrypted cell phone or laptop left in a taxi or restaurant, up to organized hacking by insider trading rings trading in clients' stocks.

2017 has brought us a comprehensive new regulation from the New York Department of Financial Services which appears to be a harbinger of things to come, as well as new ethics opinions from the organized bar emphasizing that lawyers have an ethical duty to maintain the security of electronic client confidential information. These developments are forcing law firms to be cognizant of the very real and significant risks they face in the 21st Century, and to acquire the technology sufficient to keep abreast with their clients' cybersecurity needs.