ABA Issues Formal Opinion Detailing Lawyer Obligations Relating to Cyber Attack Incidents

David J. Oberly

Law firms—more so than other business entities—are prime targets, and victims, of computer-network penetration and data theft. Law firms have access to their clients' personal information, including sensitive, heavily regulated health, financial, and proprietary business information. In addition, attorneys and firms rely heavily on computers, networks, and the storage of electronic data for their day-to-day operations. Importantly, however—even still today—the operation of law firms is generally not managed as closely or efficiently as other businesses. For the malicious hacker, then, a law firm's computer network may be much easier to penetrate than that of its clients. In addition to hackers, law firms also face significant data breach threats originating from inside the firm as well.

Cognizant of these significant risks and vulnerabilities, the American Bar Association Standing Committee on Ethics and Professional Responsibility recently released Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack," which provides detailed guidance regarding the ethical obligations that lawyers must adhere to both before and after a cyberattack occurs. Formal Opinion 483 sets a high bar in terms of lawyers' ethical obligations associated with data breaches, and as such should prompt law firms and lawyers to closely review their data breach incident preparation and response policies and procedures to ensure that they conform with their legal ethical duties.

ABA Formal Opinion 483

Formal Opinion 483 can be broken down into two distinct subparts. First, Formal Opinion 483 discusses the importance for lawyers to plan ahead and take affirmative steps to minimize the risk of falling victim to a data breach event. Model Rule 1.1—pertaining to the issue of competence—provides that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." As part of their duty of competence, lawyers are required to understand technologies that are being used to deliver services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. In addition, Rule 1.1 also imposes an ethical obligation on lawyers to take "reasonable" steps to monitor for data breaches.

Moreover, based on lawyers' obligations under Model Rules 1.1, 5.1, and 5.3 to use technology competently to safeguard confidential information against unauthorized access or loss, and to supervise lawyers and staff, Formal Opinion 483 provides that just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information. Furthermore, Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients in connection with a representation separate from the lawyer's own property.

Pursuant to Rule 1.15, a lawyer has an obligation to take reasonable precautions to safeguard client data.

Importantly, the Formal Opinion highlights the fact that while lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of economic information is not immediately detected, because cyber criminals might successfully hide their intrusion despite reasonable or even extraordinary efforts by the lawyer. Rather, 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.

Finally, with respect to lawyers' pre-breach obligations, the ABA Formal Opinion provides guidance as to best practices for minimizing the risk of negative impact to clients in the event a lawyer or law firm falls victim to a data breach incident. Model Rule 1.9(c) requires that: "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client." As a matter of best practices, lawyers are encouraged to reach agreement with clients before the conclusion, or at the termination, of the attorney-client relationship about how to handle the client's electronic information that is in the lawyer's possession. Absent an agreement with a former client, lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain.

Second, Formal Opinion 483 discusses in detail lawyers' ethical obligations that are triggered when a data breach incident is either detected or suspected. Here, the ABA cautions that mere compliance with state or federal data security laws by lawyers does "not necessarily achieve compliance with ethics obligations." Importantly, in addition to statutory data breach requirements, several ABA Model Rules are potentially implicated in connection with a breach of sensitive client data and information.

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damages resulting from the breach. The ABA recommends, as a matter of best practices, that lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach. Furthermore, after taking prompt correction to stop the breach, the duty of competence requires lawyers to make all reasonable efforts to restore computer operations to be able to service the needs of the lawyer's clients.

After a breach—pursuant to the duty of competence—attorneys must make reasonable efforts to determine what occurred during the data breach. As part of this post-breach investigatory obligation, lawyers are required to gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data that was lost or accessed.

In addition, Rule 1.6 of the Model Rules—pertaining to a lawyer's obligation to preserve the confidentiality of information relating to the representation of a client—is also implicated whenever a data breach incident occurs. Rule 1.6 was amended in 2012, and Rule 1.6(a) now provides that: "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise. The 2012 modification also added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Furthermore, Amended Comment [18] explains that the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does *not* constitute a violation of paragraph (c) if the lawyer has made "reasonable efforts" to prevent the access or disclosure.

Importantly, as indicated in the preceding paragraph, an attorney's competence in preserving a client's confidentiality is not a strict liability standard, but rather is assessed based on a "reasonable efforts" standard. As such, applied to the context of data breach incidents, Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access, including efforts to monitor for breaches of client confidentiality. Here, the ABA notes that to evaluate whether "reasonable efforts" have been deployed, a fact-specific approach will be applied to determine whether the lawyer or firm in question has engaged in a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments. Importantly, if this analysis results in a finding that such a "process" has been employed, the lawyer or firm will be found to have *not* run afoul of Rule 1.6.

At a minimum, under Rule 1.4 a lawyer must disclose to current clients that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Furthermore, lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients' information. Finally, if personally identifiable information of clients or others is compromised as a result of a data breach, the lawyer should evaluate the lawyer's obligations under state and federal law. In this regard, beyond their Rule 1.4 obligations, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.

Takeaways

Formal Opinion 483 comes directly on the heels of Formal Opinion 477R, which discusses lawyers' ethical obligations to secure client confidential data in connection with online forms of communication. The fact that the ABA has issued two formal opinions regarding the topic of data security highlights the importance lawyers and law firms must place on data protection and cybersecurity in connection with running a law practice in today's highly technological age. Formal Opinion 483 focuses on lawyers' obligations to monitor and secure electrically stored confidential client information, and their associated obligations to take affirmative action in the event a data breach incident occurs. In particular, Formal Opinion 483 provides lawyers with an

extremely useful roadmap for properly preparing for and responding to a data breach in a manner that comports with lawyers' post-breach ethical obligations.

Ultimately, Formal Opinion 483 should serve as a reminder that while the significant costs and other harm stemming from a data breach make effective long-term cybersecurity measures necessary from a business perspective, proper cybersecurity and data protection measures are also necessary from a legal ethics standpoint as well, as attorneys and law firms must satisfy certain ethical obligations directly related to the safeguarding of client information and data. In facing the growing threat of data breaches, and as legal professionals continue to embrace new and more advanced technologies, it is critical to understand and address the corresponding ethical obligations that go hand-in-hand with the use of technology in the practice of law. At the same time, Formal Opinion 483 also underscores the importance of affirmatively and effectively responding to any data breach or cyberattack incidents, and how the Model Rules come into play for legal professionals whenever a cyber event is either detected or suspected.