THE
NATIONAL LAW REVIEW

Formal Opinion 483: ABA's New Breach Notification Obligations for Lawyers and Law Firms

Wednesday, October 31, 2018

Article By
David H. Potter
Wilson Elser Moskowitz Edelman & Dicker LLP
Client Alert Communications, Media & Internet
Consumer Protection
Law Office Management
All Federal

Data breaches and cyberattacks are becoming more prevalent and law firms have quickly become attractive targets for hackers due to the sensitive and privileged information firms collect. This has prompted the American Bar Association (ABA) to release Formal Opinion 483, "Lawyers' Obligations after an Electronic Data Breach or Cyberattack." The opinion is based on the ABA Model Rules of Professional Conduct and offers guidance to attorneys to ensure reasonable steps are followed before and after a cyberattack.

The guidelines set forth in the opinion are broader than state breach notification laws and apply to any client data that may interfere with representation, instead of being limited to only personally identifiable information (PII) or personal health information (PHI). Not every cyber threat triggers the new obligations in the opinion; instead, the term breach here means a "data event where 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 by the episode." The opinion lays out a number of rules that work in concert to provide guidance to lawyers and law firms when faced with a breach of client information.

Duty of Competence

Pre-Breach: Obligation to Monitor for a Data Breach
Model Rule 1.1 sets out an attorney's duty to remain competent and "keep abreast of changes in the law and its practice," which includes understanding the basic features of technology. Further, Model Rule 5.1 and 5.3 states that lawyers have an obligation (1) to use technology competently to safeguard confidential information against unauthorized access or loss, and (2) to supervise lawyers and staff to employ reasonable efforts to monitor the technology and office resources connected to storing client information.

The opinion explains that if lawyers fail to employ such reasonable efforts, they may be unable to identify whether a breach has occurred. Therefore, just as lawyers must monitor their physical files, they must afford the same obligation and care to electronically stored digital data. The duty to monitor client information and comply with appropriate cybersecurity policies is of particular importance because cyber criminals are successful at hiding their intrusions, despite reasonable efforts taken by the firm to prevent a breach. Thus, the potential for an ethical violation does not occur when a breach is not prevented or immediately detected, but rather when a lawyer fails to undertake reasonable efforts to avoid a data loss or detect a cyber-intrusion, and the lack of reasonable efforts subsequently causes the breach.

Post-Breach: Adopting an Incident Response Plan
According to the opinion, when a breach is detected or suspected, lawyers must act reasonably and promptly to stop the breach and mitigate any damage that may have resulted. Specifically, firms also must attempt to determine what occurred during the data breach, which files were accessed and what information was compromised to determine if notification to a client is required and, if necessary, provide an accurate notification to the client. The opinion does not offer further advice on how a lawyer should accomplish this step, but instead encourages lawyers and law firms to develop an incident response plan with specific procedures in place for responding to a data breach.

An incident response plan should:

- Promptly identify and evaluate any potential network intrusion
- Assess the nature and the scope of the intrusion
- Determine if any data were accessed or compromised
- Quarantine the threat
- Prevent the exfiltration of information from the firm
- Eradicate the malware
- Restore the integrity of the firm's network.

The ABA encourages law firms and lawyers to adopt an incident response plan before any potential breach takes place. The opinion notes that incident response plans help minimize loss or theft of information by having a process in place that has prepared a firm to respond in a systematic manner to any type of cyber intrusion. If a firm chooses not to adopt an incident response plan, they are still obligated to take prompt action to stop the breach and restore computer operations.

Duty of Confidentiality

Post-Breach: Keeping Client Confidentially
Model Rule 1.6 addresses a lawyer's efforts to preserve the confidentiality of client information. The rule states that a lawyer shall not reveal information relating to the representation of a client unless certain circumstances arise. Reasonable efforts shall be made to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As previously mentioned, if an unauthorized disclosure does occur it will not automatically constitute a violation if the lawyer or firm has made reasonable efforts to prevent unauthorized access.

Comment 18 to Model Rule 1.6 lists factors to help guide lawyers in making a "reasonable efforts" determination, which include:

- The sensitivity of the information
- The likelihood of disclosure if additional safeguards are not employed
- The cost of employing additional safeguards
- The difficulty of implementing the safeguards
- The extent to which the safeguards adversely affect the lawyer's ability to represent clients.

Additionally, Rule 1.6 provides that lawyers and law firms are permitted to reveal information relating to the representation of a client if the disclosure "(a) is impliedly authorized and will advance the interests of the client in the representation, and (b) will not affect a material interest of the client adversely." It is also vital that lawyers exercise discretion when disclosing information about a breach to law enforcement, and should consider "(1) whether the client would object to the disclosure, (2) whether the client would be harmed by the disclosure, and (3) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information." In a scenario without consent, the lawyer is able to disclose only the information that is reasonably necessary in stopping the breach or recovering the stolen information.

Duty to Disclose the Breach

Post-Breach: Obligation to Notify Current and Former Clients of the Breach
Model Rule 1.4 provides that a lawyer is obligated to "keep a client reasonably informed about the status of the matter" for which the lawyer is representing the client, and it requires a lawyer to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." ABA Formal Ethics Opinion 95-398 required notification to a client when "the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation." As an example, that opinion included "where it is likely to affect the position of the client or the outcome of the client's legal matter."

Under ABA Formal Opinion 483, this notification requirement is extended to include "misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired" as a result of the breach. In light of this opinion, any time a data breach occurs that involves, or is substantially likely to involve, "material client confidential information" a lawyer has a duty to notify the client of the breach. This is mandatory to stay in compliance with the duty to keep a "client reasonably informed about the status of the matter" and to provide information "reasonably necessary to permit the client to make informed decisions regarding the representation" under Model Rule 1.4.

Interestingly, the opinion does not instruct how lawyers should disclose the event of a breach to a former client – instead the opinion simply provides that former client information shall not be revealed. This means if

unauthorized release of a former client's information does occur, Rule 1.4 does not apply in the manner it does to current clients. That being said, the opinion does encourage lawyers to either return paper files to former clients or set up a data destruction policy to avoid retaining client information indefinitely.

Post-Breach: Breach Notification Requirements
When a breach occurs and "material client information" was accessed or is reasonably suspected of having been "accessed, disclosed, or lost," a lawyer must "provide enough information for the client to make an informed decision" on how to proceed. The opinion indicates that, at a minimum, a lawyer must notify affected clients "that there has been unauthorized access to or disclosure of [client] information, or that unauthorized access or disclosure is reasonably suspected of having occurred" and advise clients of the extent of the access or disclosure. Further, the lawyer should notify the client of the firm's plan to respond to the breach. Lawyers have an ongoing duty to keep the client informed for the duration of the post-breach investigation.

It is important to remember, that if an individual's PII or PHI is compromised, a lawyer should look to state and federal privacy laws on how to proceed. The opinion maintains that lawyers should first comply with Rule 1.4 and then evaluate whether they also must comply with a separate statutory or regulatory scheme.

Summary

This opinion is primarily focused on the duty lawyers have to safeguard against breaches and the procedures to follow in the event a breach does occur. First, lawyers must properly supervise their electronic files and method of storage of client information and make a reasonable effort to prevent the unauthorized release of client information relating to a client's representation. In the event of a breach, failure to take reasonable steps to guard against cyberattacks will result in a violation. Second, should a breach occur where access to, disclosure of, or the destruction of material confidential client information occurred or likely occurred, despite a lawyer's reasonable preventive efforts, the lawyer then has a duty to notify the client of the data breach in sufficient detail to keep the client informed.

The opinion not only highlights the important obligation lawyers have to stay proactive and monitor for breaches but also takes into account the fact that cyber threats are extremely prevalent and still occur despite reasonable preventive efforts. The ABA does not provide specific instructions on how firms should monitor client information beyond the guidelines set forth in the opinion nor does it endorse any particular software. The idea behind this opinion is to make sure that lawyers, despite their attempts to limit and prevent cyber threats, are still prepared to deal with a data breach when one occurs so clients can stay informed regarding their representation. The opinion closes by stressing that lawyers are still obligated to consult the relevant regulatory and statutory schemes in addition to the model rules to fully ensure they are properly keeping their clients informed in the event of a breach.

Source URL: https://www.natlawreview.com/article/formal-opinion-483-aba-s-new-breach-notification-obligations-lawyers-and-law-firms