# The Lawyer's Duty When Client Confidential Information is Hacked From the Law Firm

**Anton Janik, Jr.**
ajanik@mwlaw.com
(501) 688.8888

03/18/2019

As attorneys, our livelihood is often heavily dependent upon the keeping of secrets. But in this complex electronic-data driven environment we work in, where physical security via locked doors and piercing alarms may no longer be solely sufficient to keep client confidences from prying eyes, what is the modern attorney supposed to do? ABA Opinion 483 provides guidance on a lawyer's duty when client confidential information is hacked from the law firm.

Imagine it's a usual Tuesday morning, and coffee in hand you stroll into your office. Right inside the door, you see a handwritten notice on a big whiteboard which says: All network services are down, DO NOT turn on your computers! Please remove all laptops from docking stations & keep turned off. *No exceptions*

Finding this odd, you turn to your firm receptionist who tells you that the firm was hit with a ransomware attack overnight, and that if you turn on your computer all of your files will be immediately encrypted, subject to a bitcoin ransom.

This really happened. In 2017, DLA Piper was hacked by the NotPetya malware, and until the breach was resolved, the 4,400-attorney law firm was reduced to conducting business by text message and cell phone.[1] The reported scope of the damage remediation included 15,000 hours of overtime IT assistance, but no reported loss of client confidential information.[2] As one of many large companies and law firms attacked by ransomware, what happened to DLA Piper was unfortunately not unique. In fact, a recent American Bar Association report stated that 22% of law firms reported a cyberattack or data breach in 2017, up from 14% the year before. [3]

Not all attacks are of the ransomware type. Some hackers are looking for specific information. Back in 2016, the Wall Street Journal reported that two major New York-based law firms were hacked in what was believed to have been a state-sponsored attack focused on front-running the equities markets by gaining advance knowledge of upcoming mergers and acquisitions.[4] Let that sink in for a minute. A foreign state hacked into U.S.-based law firms to steal confidential client data in order to front-run Wall Street on upcoming deals. If that can be done on such grand matters, who is to say it can't be done to uncover your client's real settlement posture in that next big case, or your litigation defense plan in that class action you're defending?

As attorneys, our livelihood is often heavily dependent upon the keeping of secrets, sometimes for just a short period, and other times forever. That reality is reflected in Rule 1.6 of our ethical rules, which demands that we keep secure our client confidences. But in this complex electronic-data driven environment we work in, where physical security via locked doors and piercing alarms may no longer be

solely sufficient to keep client confidences from prying eyes, what is the modern attorney supposed to do? While Arkansas has yet to issue a formal evaluation of an attorney's duty in this regard, in mid-October of last year the American Bar Association ("ABA") stepped in and issued ABA Formal Opinion 483 ("ABA Opinion"), guiding lawyers in their ethical duties to secure client data in this electronic world.[5]

The ABA Opinion answers that question through a lens centered upon the confluence of three duties under its Model Rules: the duty of competence, the duty of communication, and the duty of confidentiality. While the ABA Opinion focused narrowly upon the ethical duties it sees arising between an attorney and client, it is important that you understand the types of data you work with, and keep yourself abreast of what laws, regulations and contractual provisions govern its loss. That potential breadth is very large, and this article only briefly touches upon additional requirements that may arise under certain of those federal and state laws and regulations. (Note that the ABA Opinion points out that complying with federal and state laws and regulations does not necessarily mean that an attorney has met, or has been relieved from, the attorney's ethical obligations under the Model Rules, so you'll want to keep in mind both your ethical *and* legal duties.)

ABA Model Rule 1.1, the duty of competence, historically focused upon the need for attorneys to keep abreast of changes in the law relevant to the practice. Back in 2012, the ABA clarified Comment 8 to that Rule to sweep into such duty the requirement that an attorney keep abreast of the benefits and risks associated with technology relevant to the attorney's practice, which in 2012 terms contemplated the use of email and the creation of electronic documents. (Arkansas Rule 1.1 Comment 8 similarly states that attorneys should keep abreast of changes in the law and its practice including the benefits and risks associated with relevant technology.) Refreshing its focus on that 2012 language, in 2018 the ABA Opinion stated that once those technologies are understood, the competent attorney must use those technologies "in a manner that will reasonably safeguard the property and information entrusted to the lawyer," which may be satisfied by the attorney's own study and investigation, or by the retaining of qualified assistance. That brings us to the first ethical duty.

**1. Monitor for Electronic Data Breaches**

The ABA Opinion takes an attorney's duty of competency under Model Rule 1.1 and the duty to supervise firm lawyers and assistants under Model Rule 5.1 and 5.3 (all of which are analogous to Arkansas' provisions), and finds that an attorney has a duty to "employ reasonable efforts to monitor [for breaches] the technology and office resources connected to the internet, external data sources, and external vendors providing services related to data and the use of data."[6]

The term "breach" has many definitions, each driven by the law, regulation or rule through which an event is viewed. With regard to the ABA Opinion, a data breach is defined as "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 ABA's definition is broad enough to encompass both the situation where data is actually removed, as well as the situation where the data remains at the law firm but cannot be accessed. Turning to state law, Arkansas' Personal Information Protection Act (which is discussed more fully under the notice section below), defines a breach as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business."[7]

Recognizing the difficulty in penalizing an attorney for failing to immediately recognize a breach, especially given the sophistication that intrusion methods may employ, the ABA Opinion only finds an ethical violation where an attorney does not take reasonable efforts to avoid data loss or to detect an intrusion, and where the lack of reasonable effort was the cause of the breach. Although the ABA Opinion does not find there to be an ethical violation if the failure to reasonably act was merely a contributing factor rather than "the cause," attorneys should be careful to mitigate their exposure by making such reasonable efforts. While it is expected that most attorneys will hire specialized help to monitor for

electronic data breaches, it is recommended that complex, rotating passwords be implemented along with multifactor authentication, that all relevant security patches be installed on servers and computers, that computer logs be set to the longest retention period and depth of capture available, and that access rights and logs be regularly checked for unauthorized activity. You may want to consider software that monitors access, usage, and data flow across your internal networks, and may also consider improving physical security at the worksite and server rooms.

**2. Stopping the Breach, Restoring Systems, and Determining What Occurred**

While not formally required by the ABA Opinion, best practices (and your cybersecurity insurance coverage) dictate that your law firm should draft, and regularly train on, a breach response plan which defines personnel roles and procedural steps to employ in assessing and addressing any given breach, including through the use of outside vendors whose use may be contractually prearranged.[8] When drafting your breach response plan, keep in mind any contractual requirements your clients have established which may exceed the duties imposed under federal or state law or regulation and which may go beyond the ethical considerations of the ABA Opinion. For example, many clients require that their data be encrypted "at rest and in motion," which means while it is sitting in your law firm data repositories as well as when transmitted between that repository and any other location, for example by email or USB drive. Other clients may include requirements that the client be notified within a particular time period that differs from that required by the ABA Opinion or by state or federal law or regulation. Your breach response plan should build in those additional requirements.

When a breach is discovered, the ABA Opinion finds that the duty of competence under Model Rule 1.1 requires the attorney to act reasonably and promptly to stop the breach and mitigate the damage, using "all reasonable efforts" to restore computer operations to be able to continue client services. The ABA Opinion notes that those efforts may be undertaken through qualified personnel or experts, who should also be used to help evaluate what occurred and what can be done to prevent a reoccurrence.

Bringing in non-attorney technical expertise does raise considerations under Model Rule 1.6, the duty of confidentiality, because those personnel may come into contact with any client confidential information. As explained in ABA Formal Rule 477, an attorney's competence in preserving Model Rule 1.6 is not a strict-liability standard; rather it is an obligation to take reasonable measures.[9] Thus, Model Rule 1.6 is not abridged because a technical expert (placed under an appropriate confidentiality agreement) might come into contact with client confidential information, since reasonable efforts to secure that data may necessitate the hiring of such technical expertise. Similarly, bringing in law enforcement, including the FBI, Secret Service and state police, may be appropriate given their investigative tools and reach, and their ability to place a temporary hold on the notice requirement.

Regardless of the benefit of obtaining a temporary hold of the notice of requirement, where someone outside the attorney-client privilege is to be brought in to assist with investigation or recovery, you should have a frank discussion with your client as to each of these points and any risks that could be exposed through recovery of that data. Even with client consent, an attorney may still only disclose information specifically necessary to assist in stopping that breach or recovering that information.

**3. Providing Notice to the Client**

The requirement of notice is driven not only by the ethical rules, but also by federal and state law and regulations, and can even be driven by your client's contractual requirements. Model Rule 1.4 (and its Arkansas analogue) requires that an attorney keep the client "reasonably informed about the status of the matter." The ABA Opinion interprets that Rule to include keeping current clients informed about a data breach, because the data breach involves either the misappropriation, destruction or compromise of client confidential information, or a situation where the lawyer's ability to perform services is significantly impaired.

That disclosure must provide information sufficient for the client to make an informed decision as to what to do next, if anything. At minimum, the attorney must inform the client of the breach, even where the scope is not yet determined, and even if the breach is only reasonably suspected. The attorney should also inform the client what client confidential information was accessed. If the extent is not yet known, that should be communicated as well. Under the ABA Opinion, attorneys have a continuing duty to keep their clients reasonably apprised of material developments in the post-breach investigation that affect client information.

The ABA's Opinion does not extend to alerting prior clients of a breach because, as written, Model Rule 1.9 (and its Arkansas analogue) fails to describe what steps a lawyer must take if a former client's data is revealed. While that approach may make sense in the context of a ransomware attack where an attorney cannot work on a current client's matter, in the case of a loss of data this approach does not appear to fully appreciate the realities of modern law practice, where electronic client confidential information may be housed at the law firm or in its repositories for years beyond the conclusion of a particular matter, and perhaps even beyond any relevant statute of limitations. Regardless of a lack of a written Model Rule requirement, you should provide notice to former clients whose confidential information has been compromised, and establish paper and electronic document destruction policies that require confidential client information to be securely destroyed after an appropriate interval.

Outside of the ethical notice requirements, disclosure to regulators and those affected is driven by federal and/or state regulation and law. In that context, similar to the ethical rules which are triggered when client confidential information is at issue, the duties to provide notice are controlled by the type of data breached. For example, under HIPAA, the loss of "protected health information"—in short, information relating to medical diagnoses or care—triggers the requirement to provide notice.[10] Under Arkansas state law, the Personal Information Protection Act ("PIPA") requires notice to those affected if there is a loss of data that includes at least the first initial of the first name and the last name of a person, along with any of several data variants: social security number, driver's license number, financial account or credit card number and password, or medical information.[11] It is important to note that even if the ethical duty to investigate and provide notice is not triggered because no client confidential information was compromised, other data in your repositories may trigger the duty to investigate and provide notice under relevant federal or state laws or regulations.

Under HIPAA, you generally have up to 60 days to provide notice to affected persons.[12] Under PIPA, the disclosure must be made "without unreasonable delay," which may take into account a request by law enforcement to delay notice due to investigative actions.[13] When considering your requirements, be sure you are considering the local law of the state of residency of those whose data is affected, regardless of the fact that the loss may have occurred only here in Arkansas. States differ in their notice requirements and in their required breach response steps, and those laws apply to their residents' data regardless of where the breach actually occurs.

This article is necessarily concise, and has only lightly touched upon several of the relevant considerations. Keep in mind that the ABA has framed these responsibilities as ethical duties, and that Arkansas has already adopted the relevant language from the Model Rules. Arkansas has not provided guidance on the duties raised in ABA Opinion 483. If Arkansas adopts the reasonings of ABA Opinion 483, attorneys will need to proceed carefully, because violations of the ethical duties can lead to sanctions far in excess of the financial sanctions imposed under federal and state laws and regulations.

***Endnotes:***

1. *See* https://www.abc.net.au/news/2017-06-28/ransomware-virus-hits-computer-servers-across-the-globe/8657626 (last visited January 6, 2019).

2. *See id.*

3. *See* https://www.lawyersmutualnc.com/blog/one-in-5-law-firms-hacked-in-2017 (last visited January 6, 2019).

4. *See* https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504 (last visited January 6, 2019). *See also* FBI Private Industry Notification 160304-001, available at https://info.publicintelligence.net/FBI-InsiderTradingHacking.pdf (last visited January 6, 2019).

5. American Bar Association, Formal Opinion 483, available at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf (last visited January 6, 2019) ("ABA Opinion").

6. ABA Opinion, at 5.

7. Ark. Code Ann. § 4-110-101, *et seq.*

8. *See* M. Stanton, et al., Cybersecurity Best Practices, 51 *The Arkansas Lawyer* 4 (2016), for a deeper discussion of the elements of a breach response plan.

9. American Bar Association, Formal Opinion 477, available at https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf.

10. 46 C.F.R. § 164.04(a)(1).

11. Ark. Code Ann. § 4-110-103(7).

12. 45 C.F.R. § 164.404 (b).

13. Ark. Code Ann. § 4-110-105(c).n

*Republished with permission. This article was originally published in the 2019 Winter issue of The Arkansas Lawyer.*