THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
COMMITTEE ON PROFESSIONAL ETHICS

FORMAL OPINION 2024-3: ETHICAL OBLIGATIONS RELATING TO A CYBERSECURITY INCIDENT

TOPIC: Lawyers' ethical obligations in the event of a cybersecurity incident or cyber extortion demand that compromises, or threatens to compromise, client confidential information or prevents a lawyer from accessing client information or operating systems.

DIGEST: When a cybersecurity incident occurs at a law firm that compromises, or threatens to compromise, client confidential information or prevents a lawyer from accessing client information, the New York Rules of Professional Conduct (the "Rules") guide a lawyer's or law firms' actions in responding to the incident:

- Lawyers and law firms have an obligation of technological competence under Rules 1.1, 1.3 and 1.6 to take appropriate steps to protect clients' confidential data.

- In the wake of a cybersecurity incident, lawyers and law firms may have statutory, regulatory, or contractual obligations to notify clients and other third parties. Separate from and in addition to those obligations, lawyers and law firms have an ethical obligation under Rule 1.4 to promptly notify current clients when a cybersecurity incident occurs that constitutes a "material development" in a representation or must be explained to the client to permit the client to make an informed decision regarding the representation. Although Rule 1.4 does not require notification to former or prospective clients, lawyers may decide, where reasonable, to notify former or prospective clients who are likely to have been harmed as a result of the loss or theft of their sensitive confidential information in a lawyer's or law firm's cybersecurity incident.

- If a lawyer or law firm chooses to negotiate with the cyber-extortionists in order to regain system access or protect client information, generally accepted conventions, as well as the underlying rationale of Rules 4.1 and 8.4(c), public policy and the societal good, permit being not candid to those cyber-extortionists about facts relating to the impact of the cyber attack, the victim's financial situation, and any actions taken to mitigate the damage caused by the attack.

- While not a common occurrence, in situations where a lawyer or law firm receives advance notice of an impending cybersecurity attack through a threat by the cyber-extortionist, a lawyer or law firm must take reasonable efforts to determine the nature of the threat and what, if any, actions the lawyer or law firm can take to prevent or ameliorate any effects to client information or to the lawyer's ability to competently and diligently represent clients. Rule 1.4 does not require current clients be notified of the cyber threat; however, if the lawyer or law firm reasonably believes that it may have to push back important meetings or events (*e.g.*, an imminent deal closing, start of trial, or a deposition) for certain client matters because of the likely effects of a credible cyber threat

on its ability to perform the necessary work, the lawyer or law firm should promptly inform the affected clients that emergent circumstances have arisen and advise them of the efforts that the firm is taking to reschedule those meetings or events.

- When a lawyer or law firm is the victim of a cybersecurity incident, there is no ethical prohibition against paying, or obligation to pay, a ransom.

- Rule 1.7 may prohibit lawyers or law firms from continuing to represent (or from taking on a new representation of) a client whose confidential information has or may be compromised in a cybersecurity incident if (1) the client's obligations to or interest in further reporting the cybersecurity interest differ from the lawyer's or law firm's interests; or (2) the client may have a claim or has expressed that it may have a claim of malpractice or breach of fiduciary duty against the lawyer or law firm as a result of the cybersecurity incident.

- A lawyer or law firm that is the victim of a cybersecurity incident and wishes to report it to law enforcement or cooperate in a governmental investigation into the incident must be cognizant of its continuing confidentiality obligations to current, former, or prospective clients under Rules 1.6, 1.9 and 1.18, and of the potential adverse effects to the clients that may result by reporting information to the government. In making a disclosure to the government, the lawyer should consider whether it should: (1) report the incident but not disclose the clients whose files were taken or other confidential client information; or (2) obtain consent from the affected clients, former clients or prospective clients to the disclosure of client confidences to the government; or (3) limit disclosures to those client confidences that are reasonable and impliedly authorized to advance the best interests of the clients, such as by stopping an ongoing breach or recovering a clients' confidential information.

RULES: 1.1, 1.3, 1.4, 1.6, 1.7(a)(2), 1.9, 1.15, 1.18, 4.1, 5.1, 5.3, 8.4

QUESTION: What are a lawyer's ethical obligations in the event of (i) a cybersecurity incident that compromises, threatens to compromise, or prevents a lawyer from accessing client confidential information, or (ii) a cyber extortion demand that unless a ransom is paid the extortionist will misappropriate or leak client information and/or disrupt the law firm's ability to represent clients by shutting down the firm's systems or keeping the firm locked out of its systems?

OPINION:

Introduction

This opinion addresses lawyers' and law firms' ethical obligations, particularly to clients, when a lawyer or law firm experiences a cybersecurity incident. The National Institute of Standards and Technology's (NIST) Computer Security Resource Center defines a cybersecurity "incident" as "an occurrence that actually or potentially jeopardizes the confidentiality, integrity,

or availability[1] of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."[2] The nature and method of attack that leads to such incidents are varied.

An example of a confidentiality incident is the series of attacks experienced in May 2023 by hundreds of organizations, including law firms, as a result of the "zero day" vulnerability in the MOVEit secure file transfer application. In that attack, the threat actor was able to exploit the vulnerability and exfiltrate (*i.e.*, steal) large amounts of sensitive data of those organizations. The types of data affected differed by victim organization, but often included sensitive personally identifiable information of individuals (*e.g.*, national ID numbers, names, financial data, health data), trade secrets, formulas, and competitive data.[3]

An example of an integrity incident is an attack against a financial institution that enables a threat actor to alter, delete, or otherwise affect the values of account balances.

An example of an availability incident is a Distributed Denial of Service (or "DDoS") attack. According to Microsoft, "a DDoS attack targets websites and servers by disrupting network services in an attempt to exhaust an application's resources. The perpetrators behind these attacks flood a site with errant traffic, resulting in poor website functionality or knocking it offline altogether."[4] The result is that the victim firm is frozen or locked out of its systems, effectively shutting down all of its work.

Unfortunately, lawyers and law firms are not immune from these attacks – whether a confidentiality incident, integrity incident, availability incident, or any combination of the three –

---

[1] The NIST definitions of confidentiality, integrity, and availability are:

- Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. https://csrc.nist.gov/glossary/term/confidentiality.
- Integrity: Guarding against improper information modification or destruction and includes insuring information non-repudiation and authenticity. https://csrc.nist.gov/glossary/term/integrity.
- Availability: Ensuring timely and reliable access to and use of information. https://csrc.nist.gov/glossary/term/availability (All websites last accessed on July 15, 2024).

[2] The NIST definition of incident is:

- Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. https://csrc.nist.gov/glossary/term/incident#:~:text=An%20occurrence%20that%20actually%20or,security%20procedures%2C%20or%20acceptable%20use.

[3] Jonathan Reed, *The MOVEit breach impact and fallout: how can you respond?*, SECURITYINTELLIGENCE, July 19, 2023 (https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/).

[4] Microsoft, 'What Is a DDoS Attack?', Microsoft Security, https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack

and they continue to occur despite reasonable efforts to safeguard computer systems and client data.

In 2024, the most common type of cybersecurity incident that organizations face is a ransomware attack. The United States Cybersecurity & Infrastructure Security Agency ("CISA") describes ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."[5] Ransomware attacks can be availability incidents, confidentiality incidents, or a combination of both. In cyber extortion cases such as the MOVEit attacks mentioned above, a threat actor may decide to skip the encryption step and focus solely on the data exfiltration component of the attack, threatening to sell or leak the data if the ransom is not paid.

I. Duties to Protect Client Data and Monitor for Cyber Incidents that Threaten Confidential Information or the Representation of the Client

The Standing Committee on Ethics and Professional Responsibility of the American Bar Association ("ABA") and other bar associations have addressed lawyers' duties of competence and confidentiality in connection with using, maintaining, and protecting client information in their possession, including from cybersecurity incidents. In light of these duties, the opinions conclude that lawyers are obliged to:

- understand the technologies used to deliver legal services to clients;
- "use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer";
- monitor for cyber incidents where "material client confidential information" may be "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 incident;
- undertake reasonable and prompt efforts to investigate cyber incidents that occur in order to ensure the intrusion has been remediated and to determine what data was lost, stolen, or accessed; and
- take reasonable steps to mitigate certain harm that may result from an incident.

ABA Formal Op. 483 (2018) at 3-8; *see also* California Opinion 2020-203 at 3-4; Colorado Opinion 141 (2020) at 2 ("A lawyer must make reasonable efforts to prevent, monitor for, halt, and investigate any security breach of data the lawyer controls.").

[5] Cybersecurity and Infrastructure Security Agency (CISA), 'Ransomware 101,' https://www.cisa.gov/stopransomware/ransomware-101#:~:text=Ransomware%20is%20an%20ever%2Devolving,ransom%20in%20exchange%20for%20decryption.

We agree and adopt the ABA's analysis in its Formal Opinion 483 of these obligations, as summarized above, based upon lawyers' duties of competence and confidentiality.[6] Comment 8 to Rule 1.1 of the New York Rules notes that to maintain the requisite knowledge and skill to competently represent a client, "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 . . . ."[7] Rule 1.6(c) requires a lawyer "to make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c) or 1.18(b)." Rule 1.3(a) requires lawyers to act with "reasonable diligence and promptness in representing a client."

Likewise, consistent with Rules 5.1 and 5.3, lawyers and law firms must make reasonable efforts to ensure that cybersecurity policies and procedures designed to reasonably monitor technology resources and safeguard client data are followed by all lawyers and nonlawyers at the firm, as well as, where reasonable, to conduct appropriate due diligence and monitoring of data security controls in place for any outside vendors retained by the law firm in connection with the storage, management, transfer, or other use of client information. Rules 1.6, 5.1 and 5.3; ABA Formal Op. 483 at 5; Michigan Opinion RI-381 (2020).[8]

Indeed, it is often necessary or advisable for lawyers and law firms to engage outside vendors with the necessary technical expertise to ensure client information stored, managed, or transferred on the lawyer's or law firm's systems is secure, as well as to identify, investigate, halt, or otherwise respond to a cyber incident. The Rules contemplate this type of nonlawyer assistance, which is ethically permissible provided that the lawyer or law firm makes reasonable efforts to ensure the vendors' services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm, including under Rule 1.6. *See* Rule 1.6(c); Rule 5.3(a), cmt. [2] ("A law firm should make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that … nonlawyers outside the firm who work on firm matters will act in a way compatible with the professional obligations of the lawyer.").

The extent of reasonable efforts required will depend upon the circumstances, including the nature of the services involved, the terms of any arrangements concerning the protection of client information, and the sensitivity of the particular kind of confidential information at issue. *See* Rule 5.3(a), cmt. [3]. In the case of vendors who assist with the storage, management or transfer of client information or with the investigation and response to a cyber incident, "reasonable efforts" under Rule 5.3 would include (1) requiring the vendors' treatment of

[6] The ABA Formal Op. 483 analysis also comports with the analysis of New York ethics opinions on similar technology related issues. *See, e.g.,* New York State Opinion 842 (2010) (discussing a lawyer's obligations in using an online data system to store client confidential information).

[7] In 2023, New York became the first state to require that lawyers, to fulfill their continuing legal education obligations, have one hour of training ever two years on cybersecurity.

[8] These obligations only require reasonable efforts, which may vary based on the size of the law firm and the matters that the lawyer or law firm is handling. We believe that, particularly for smaller law firms or solo practitioners, it may not be reasonable to conduct the same level of due diligence on their vendors that a large law firm with a different risk profile may be required to do. For example, we think it may be reasonable for a smaller law firms or solo practitioners to rely on the stated security features of well-known or industry leading vendors (*e.g.*, Google, Microsoft, Apple) without doing additional due diligence.

confidential information to be compatible with the lawyer's Rule 1.6 obligations; and (2) limiting access to client information to only that reasonably necessary for the vendors to effectively perform their services.

II. Obligations to Notify Current Clients Following a Cybersecurity Incident

A host of privacy laws and other regulations in the United States and globally impose notification obligations on lawyers and law firms in the event that a cyber incident involves a data breach. A "data breach" has been defined as "any security incident in which unauthorized parties gain access to sensitive data or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information)."[9] Data breach laws and regulations differ in terms of timing, triggers, and data elements requiring notification. A firm may need to comply with the laws of multiple jurisdictions, requiring a jurisdiction-by-jurisdiction analysis of applicable laws and potentially application of the laws of foreign jurisdictions, such as the European Union's General Data Protection Regulation. In addition, client engagement terms or other contractual obligations may require notification of a data breach or other cyber incidents under circumstances specified in the contract.[10]

However, this Committee's opinion on a lawyer's obligations to notify a client is limited to obligations that the Rules may impose, separate and apart from the potential myriad of statutory, regulatory, or contractual obligations a lawyer may have in the wake of a cyber incident. New York lawyers are ethically obligated to "promptly inform" a client of "material developments" in a matter, keep clients "reasonably informed about the status of [a] matter," and "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Rule 1.4(a)(1)(iii), (a)(3) and (b). These notification obligations only apply to a lawyer's current clients.[11] The question is whether and when the occurrence of a cyber incident,

---

[9] IBM, 'Data Breach,' https://www.ibm.com/topics/data-breach. The term "data breach" is a legal term of art that is often used interchangeably with a cyberattack or cybersecurity incident but should not be. Not every cybersecurity incident results in a data breach, and there are many types of data breaches that do not have a cybersecurity nexus (*e.g.*, a law firm sends Client A's information to Client B).

[10] Outside counsel guidelines issued by corporate entities sometimes address a law firm's obligations to report on cybersecurity incidents and/or data breaches. Law firms should carefully review these provisions before agreeing to them. For example, to the extent that these provisions purport to require disclosure of the confidential information of other clients, the provision will run afoul of Rule 1.6. Law firms also may wish to consider whether to agree to provisions that require disclosure of all cybersecurity threats or to require disclosure before the law firm may have had a reasonable time to consider the scope of a cybersecurity incident or data breach.

[11] *See* ABA Formal Op. 481 (2018) ("Nowhere does Model Rule 1.4 impose on lawyers a duty to communicate with former clients . . . . Had the drafters of the Model Rules intended Rule 1.4 to apply to former clients, they presumably would have referred to former clients in the language of the rule or in the comments to the rule."), and New York City Opinion 2023-1 (Client notification is required when an attorney departs a law firm, but noting that while "Comment [7A] to Rule 1.4 requires notice to be sent to all *current* clients [in certain situations]…. [t]he Rules do not expressly address the issue of notice to anyone else." (emphasis added)). It should be noted that there are some ethics opinions which appear to have read Rule 1.4 to apply to communications with *prospective* clients to ensure that they fully understand the nature of the relationship they will be entering with the lawyer. New York City Opinion 2017-7 (requiring lawyers to generally "advise prospective joint clients of the implications of the joint representation" where appropriate); ABA Formal Op. 02-425 (2002) ("The Committee is of the opinion that Rule

and its impact on the client's confidential information, representation, or other interests constitutes a "material development" that must be disclosed to the client or one that needs to be explained to the client to permit it to make an informed decision regarding the representation.

It is important to recognize that a lawyer's notification obligations under the Rules may be entirely different than those imposed by contract or by local, state, federal or international law, including to whom notification must be provided, the information that must be disclosed, and the timing of the notification or disclosure. These distinctions are critical, and a lawyer cannot assume that fulfilling notification requirements under the Rules will fulfill any or all statutory or contractual obligations, or that fulfilling statutory or contractual obligations will necessarily fulfill ethical obligations. Each must be considered separately.

A. Incidents that compromise the confidentiality of current client information

When a cybersecurity incident occurs that compromises, or has a substantial likelihood of compromising, confidential information of a current client, Rule 1.4 may require lawyers to promptly[12] notify current clients of the facts and circumstances of the incident, including what data are believed to have been exfiltrated, destroyed, accessed, or otherwise compromised. Lawyers should also inform the clients of the efforts the lawyers have made and intend to make to recover, restore, and protect client data from further unauthorized access.

This conclusion is consistent with other New York ethics opinions on the duty to notify clients when confidential information has been destroyed, stolen, or subject to unauthorized access. *See* New York City Opinion 2017-5 (if a lawyer's electronic device containing client confidential information is reviewed or seized in a U.S. border search, the lawyer must promptly notify affected clients of what occurred and the extent to which their confidential information was affected); New York City Opinion 2015-6 (lawyers have a duty to promptly notify clients if certain material files have been inadvertently destroyed); New York State Opinion 842 (a lawyer must notify affected clients of any breach of client confidentiality by a cloud storage provider used by the firm).[13]

However, the compromise of a current client's confidential information does not require notification in all circumstances. Where the information compromised was obtained by the lawyer as part of a current matter for that client, a breach in the client's confidences, regardless of the materiality of the compromised information, will always require notification under Rule 1.4. By contrast, where the confidential information was obtained during a prior representation of a current client, the obligation to notify that current client only arises where the compromise of such

1.4(b) applies when lawyers ask prospective clients to execute retainer agreements that include provisions mandating the use of arbitration to resolve fee disputes and malpractice claims."). To the extent that Rule 1.4 may require such communications with prospective clients in that context, the committee is of the opinion that Rule 1.4 obligations do not apply to prospective clients whose confidential information may have been compromised.

[12] *See* discussion in Section II, Part D below on what "promptly" means.

[13] Other ethics opinions have come to a similar conclusion. *See* ABA Formal Op. 483 at 11; California Opinion 2020-203 (2020) ("misappropriation, destruction, or compromising of confidential client information . . . is a 'significant development' that must be communicated to a client"); Kentucky Opinion E-446 (2018) (same); Michigan Opinion RI-381 (2020) (a lawyer has a duty to inform a client in a timely manner of a data breach that "involves unauthorized access, destruction, corruption, or ransoming" of confidential client information; "[t]he duty to inform includes the extent of the breach and the efforts made and to be made by the lawyer to limit the breach").

confidential information could affect the client's interests in a current matter. Otherwise, Rule 1.4 is not implicated.[14] For example, if a lawyer is representing a long-time client in a divorce proceeding, a lawyer would have to notify that client if sensitive financial information obtained in a prior representation is compromised if that information could be relevant to the divorce proceeding. By contrast, if the information compromised in the cybersecurity incident related to an old drunk driving matter that has no relevance to the divorce proceeding, the lawyer would not have an obligation under Rule 1.4 to notify the client.[15] It may be hard to determine whether information obtained during a prior representation could affect a client's interest in a current matter. While there can be no bright-line test, a lawyer may wish to consider erring on the side of caution and providing notification to the current client.

B. Incidents that compromise the availability of client information but may not have compromised the confidentiality of client information

Where an incident prevents the law firm from accessing client information – but where the lawyer does not know that client information has been compromised – the Rules obligate lawyers to take reasonable steps to determine the scope of attack and restore access, as discussed in Section I above. However, the law firm may not be ethically required to provide any notice to clients in such circumstances unless the lack of access to the information materially impairs the client's interests or the lawyer's ability to represent the client competently and diligently. We agree with the ABA and other bars that have concluded that a cybersecurity incident that *materially* impairs the lawyer's ability to provide legal services to clients is a "material development" in a matter about which the lawyer must "promptly inform the client" and explain the facts and circumstances to the extent "reasonably necessary to permit the client to make informed decisions regarding the representation." Rule 1.4(a)(iii) and (b). *See also* ABA Formal Op. 483 at 10; California Opinion 2020-203 at 6 ("a cyberbreach that has significantly impaired the lawyer's ability to provide legal services to clients, is a 'significant development' that must be communicated to a client"); Kentucky Opinion E-446 (2018) (same); Michigan Opinion RI-381 (a lawyer has a duty to inform a client in a timely manner of a data breach that "materially impairs the lawyer's ability to perform the legal services for which the lawyer has been hired").

C. Obligations to clients when a cybersecurity incident is threatened but the incident has not yet occurred

Unfortunately, by the time a lawyer or law firm realizes that they are the victim of a cybersecurity attack – *e.g.*, when they receive a ransom note – key systems/files (and, importantly, their backup systems) are usually already encrypted. However, while not a common occurrence, there may be situations where a lawyer or law firm receives advance notice of an impending cybersecurity attack through a threat by the cyber-extortionist.

[14] There may be many other reasons why a lawyer may want to notify a client of the breach even if not required to under the Rules. For example, we think that, where the lawyer has a reasonable opportunity to do so, the lawyer should consider notifying the current client as a matter of professionalism.

[15] This is true even though the disclosure of the drunk driving matter might harm the client's reputation or cause the client financial harm.

Consider a scenario in which a law firm receives a cyber extortion threat at 6:00 p.m. on a Friday, demanding payment in 3 days. The extortionist threatens that, if payment is not received, the firm will be locked out of its own computer systems, unable to access any of its files. The law firm's investigation reveals that the threat is from a group of cyber criminals with a proven track record of following through on its threats. The law firm believes that based on its current capabilities and the timing, it will not be able to prevent the cyberattack on its computer systems or successfully "unlock" the systems after the attack. The law firm has also determined that the threat is credible based upon some indication of breach or evidence of data extraction. The law firm decides, however, to not make a payment to the cyber-extortionists.[16]

Rule 1.6(c) requires lawyers to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b)." Thus, where a lawyer or law firm has some sort of advance notice that clients' confidential information may be compromised or affected in a cybersecurity incident, including a threat in the form of an extortionate demand, the lawyer or law firm must make reasonable efforts to determine the nature of the threat and what, if any, actions the lawyer or law firm can take to prevent or ameliorate any effects to client information. Furthermore, a lawyer's continuing obligations to provide competent representation under Rule 1.1 may require the lawyer to take additional steps to lessen any potential harm from the cyberattack.

The lawyer or law firm may choose to take preemptive steps on a confidential basis to comply with its ethical obligations in the scenario described above, for example, by copying the relevant client files to a system that will not be affected by the cyberattack and communicating with law enforcement. The law firm also may decide to preemptively retain outside legal and technical assistance (*see* Section I above) to help with responding to the threat and coordinating with law enforcement (*see* Section VI below).

To maintain confidentiality and manage the threat response, the lawyer or law firm may decide to limit disclosure of the threat to third parties, including clients. This Committee concludes that Rule 1.4 does not require in this scenario that current clients be notified of the cyber threat. However, if the lawyer or law firm reasonably believes that it may have to push back important meetings or events (*e.g.*, an imminent deal closing, start of trial, or a deposition) for certain client matters because of the likely effects of a credible cyber threat on its ability to perform the necessary work, the law firm should promptly inform the affected clients that emergent circumstances have arisen and advise them of the efforts that the firm is taking to reschedule those meetings or events. *See* Rule 1.4(a)(1)(iii). It is not ethically required that the details of the emergent circumstances be disclosed; if a client pushes for further details, it is sufficient to indicate that the reasons are confidential.

D. Timing of notification to clients

There remains a question of timing. What does "promptly" mean in the context of the ethical duty to notify a client of a cyber incident? The term is not defined in Rule 1.4 or elsewhere in the rules. The varying nature of cyber incidents, the investigation required when one is identified or suspected, and the need to mount an immediate incident response makes the timing of

[16] A lawyer or law firm may also choose to pay the ransom demand as discussed in Section IV below.

notification difficult to define with specificity or a general bright-line rule. When a lawyer or law firm experiences a cybersecurity incident, among the many priorities will be determining whether the attack resulted in a data breach as defined under applicable statutory or regulatory law.This determination will be informed by the results of a forensic investigation, ideally conducted by a reputable cybersecurity incident response company and perhaps under the oversight of outside counsel. A lawyer or law firm may also feel the need to consult with law enforcement (without necessarily disclosing client confidences, like the identity of any potentially affected clients, *see* Section VI below) before notifying any third party, including clients, of the breach or threat. Depending on the scope of the incident, those investigations may take weeks or even months.

For a lawyer or law firm to fulfill their obligation to notify current clients of cyber incidents under Rule 1.4, some investigation is likely to be necessary in order to identify the clients whose confidential information is likely to have been impacted and to determine whether an accessibility incident has impacted the ability of the firm to carry out the representation of the client competently and diligently. As noted above, notification obligations under data breach laws, and the timing of those notifications, are not necessarily the same as those under Rule 1.4. It is entirely possible, based upon the circumstances, that a lawyer will have sufficient information to provide a current client with the relevant Rule 1.4 notification long before any similar or additional notifications must be made under a statute or regulation. The reverse is also true: the triggering event and timing for notification under statute, regulation, or contract may occur before the firm has determined that the event has actually impacted a current client either in terms of exposure of confidential information or the ability to carry out the representation so as to trigger a Rule 1.4 obligation.

This Committee has defined "promptly" in the context of other notification obligations. With respect to inadvertent disclosure of documents, the Committee defined the obligation of a lawyer to notify the sender "promptly" under Rule 4.4 as meaning "as soon as reasonably possible, as the rule is designed in part to eliminate any unfair advantage that would arise if the lawyer did not provide such a notice." New York City Opinion 2012-1. This Committee also addressed a prosecutor's obligation under Rule 3.8(b) to make a "timely disclosure" to defendant of evidence or information known to the prosecutor that tends to negate the guilt of the accused, noting that timeliness is used in the Rules interchangeably with, and without distinction to, the term promptness. New York City Opinion 2016-3. It noted that the term is "equated with 'as soon as practical' in situations where the duty in question is established by the Rules themselves, not exclusively by other law." *Id.* The Committee concluded that timeliness "depends upon the purposes for which the disclosure must be made" and, in the context of a prosecutor's obligation under Rule 3.8(b), that means early enough that the information can be used effectively by the defense, "which will ordinarily be before trial." *Id.* citing ABA Formal Op. 09-454 at 6.

The reasoning underlying these prior opinions applies to the question of what constitutes a "prompt" notification to a client of a cyber incident under Rule 1.4. Notwithstanding specific disclosure requirements under applicable law that may require an earlier or later notification, we conclude that notification to a current client under Rule 1.4 should be made at the earliest time after a cybersecurity incident has been identified and the lawyer has enough information about the incident to determine whether and how the client's confidential information has or may be affected or that the representation of the client has been negatively impacted by an availability incident. Where it is reasonable to do so, the lawyer or law firm should endeavor to provide notice at a time

early enough for the client to be able to make informed decisions about how to protect its interests, including its legal representation, in light of the threats that the cybersecurity incident poses.

III. Obligations to Notify Former or Prospective Clients

As discussed above, lawyers may be obligated to provide certain notifications required by law,[17] regulation, or contract to former clients, prospective clients or third parties whose confidential information was compromised. However, in contrast to the obligation to notify current clients under Rule 1.4, there is no similar ethical obligation to notify a lawyer's former clients or prospective clients under the Rules in most circumstances.

Rule 1.9(c), which governs a lawyer's confidentiality obligations to a former client, provides that a lawyer should not "use confidential information of the former client protected by Rule 1.6 to the disadvantage of the former client" or "reveal confidential information of the former client protected by Rule 1.6" except where the Rules would otherwise permit. Rule 1.9(c)(1) and (2). Similarly, Rule 1.18(b), which governs a lawyer's confidentiality obligations to a prospective client, states that "a lawyer who has learned information from a prospective client shall not use or reveal that information, except as Rule 1.9 would permit with respect to information of a former client." Neither Rule discusses notification obligations, nor do we believe that the Rules intended for such a result here.[18]

This is not to say that there are no circumstances in which a lawyer may be ethically required to notify a former client (or prospective client) of a cybersecurity incident affecting their confidential information, such as under Rule 1.15(c) obligations to safeguard and account for property belonging to another person.[19]

Even where a lawyer is not obligated under the Rules to do so, lawyers may certainly decide, where reasonable, to provide notifications to former or prospective clients who are likely to have been harmed as a result of the loss or theft of their sensitive confidential information in a cybersecurity incident.

---

[17] This includes possible fiduciary obligations to a former client if the lawyer has retained that former client's files. *See* Rule 1.15(a) (" A lawyer in possession of any funds or other property belonging to another person, where such possession is incident to his or her practice of law, is a fiduciary…"); *Sage Realty Corp. v. Proskauer Rose Goetz & Mendelsohn LLP*, 91 N.Y.2d 30, 37 (1997) ("an attorney's fiduciary relationship with a client may continue even after representation has concluded").

[18] Other ethics committees examining this issue have come to the same conclusion. *See* ABA Formal Op. 483 (2018) ("The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice."); Colorado Opinion 141 (2020) (same); *but see* Maine Opinion 220 (2019) ("A former client must be timely notified regarding a cyberattack or data breach that has, or may have, exposed the client's confidences or secrets.").

[19] For example, in New York City Opinion 2015-6, this Committee concluded that if certain original documents, such as "wills, deeds and negotiable instruments," are destroyed in an accident or disaster such as a warehouse fire, lawyers may have an obligation to notify both current and former clients of the destruction of those documents under Rule 1.15.

IV. Making Ransom Payments to Cyber-Extortionists

As discussed above, cybersecurity incidents may involve a threat actor demanding payment from a victim organization in order to restore computer systems or to refrain from disclosure of confidential information. The federal government discourages paying ransoms based upon concerns that the payments incentivize future attacks and that there is no guarantee data will become accessible or that further attacks will not ensue. However, the Committee is not aware of any federal or state laws that expressly prohibit or make illegal payment of a ransom unless the party to be paid is a foreign terrorist organization or subject to sanctions by the Department of Treasury through the Office of Foreign Assets Control ("OFAC").[20] In such a case, there is a risk that a firm will be subject to civil or criminal sanctions. Given the possibility that a ransom payment could result in civil or criminal sanctions under OFAC regulations, does a decision to negotiate with a threat actor and to pay a ransom violate the prohibitions in Rule 8.4(b) and (h) against engaging in illegal or any other conduct that adversely reflects on the lawyer's honesty, trustworthiness, or fitness as a lawyer? While lawyers should very carefully weigh whether payment of a specific ransom could result in sanctions and not take the decision whether to pay such a ransom lightly, we conclude it does not.

As noted in the commentary to Rule 8.4, many types of illegal conduct can reflect adversely on a lawyer's fitness to practice law, such as those involving "violence, dishonesty, fraud, breach of trust, or serious interference with the administration of justice." Rule 8.4, cmt. [2]. Paying a ransom to a threat actor in order to safeguard client information or permit the firm to continue to represent its clients does not reflect adversely on a lawyer's honesty, trustworthiness, or fitness to practice law, even if the payment ultimately is not in compliance with applicable laws or regulations. In these scenarios, the law firm is the victim, not the perpetrator, of a crime. The goal of the firm in paying a ransom is not to defraud, breach a trust, or otherwise act indifferently to legal obligations, but instead to recover its business and client information or its operating systems that the threat actor holds hostage.

Thus, the Committee believes that the payment of a ransom to recover the firm's operating systems and/or client information is not a violation of Rule 8.4.[21]

Conversely, the Committee does not believe that any of the Rules *obligate* a lawyer or a law firm to pay a ransom in order to recover its systems or to attempt to block further disclosure of client data, even if the payment is small or if a client offers to pay it on the lawyer's or law

[20] In 2021, OFAC issued an advisory on these heightened sanctions risks associated with ransomware payments, explaining that victims who pay ransoms to individuals or to entities or digital currency addresses listed on the Specially Designated Nationals and Blocked Persons List ("SDN list") or to countries or regions under embargo, such as Cuba, Crimea, Iran, North Korea, and Syria may be subject to civil penalties for sanctions violations based upon strict liability or criminal liability if the payment is knowingly made to a foreign terrorist organization. https://ofac.treasury.gov/recent-actions/20210921.

[21] Lawyers may also ask clients to contribute to ransom payments. If a lawyer enters into such a financial arrangement with a client, the lawyer should be cognizant of and comply with the requirements of Rule 1.8(a).

firm's behalf.[22] As the victim of the cybersecurity incident, the lawyer or law firm must make its own informed decisions on how to respond.

V. Using Deception When Negotiating with Cyber-Extortionists

New York lawyers are ethically prohibited from "knowingly making a false statement of fact or law" to a third person in the course of representing a client (Rule 4.1) and, more broadly, from engaging in conduct involving dishonesty, fraud, or deceit, even if not representing a client (Rule 8.4(c)). Lawyers are also prohibited from violating their ethical obligations under the Rules through the acts of another or knowingly assisting or inducing another to do so. Rule 8.4(a). Thus, lawyers in most cases are ethically proscribed from lying to another party or directing an agent to do so.[23]

The black letter text of Rule 8.4(c) does not contain any exceptions and, read literally, applies to all of a lawyer's conduct, whether in the context of the practice of law or not. This is for good reason: it is necessary to hold lawyers to a high standard of honesty to ensure the public's confidence in the profession and in the judicial system as a whole. However, one must look to the underlying rationale of a rule in construing its applicability to certain situations.[24] As such, the comments to the Rules, as well as prior opinions by this Committee (and other ethics committees) have found that certain deceptive or less than forthcoming conduct by lawyers is permissible in specific and limited situations.

Comment [2] to Rule 4.1 clarifies that "[u]nder generally accepted conventions in negotiation, certain types of statements ordinarily are not taken as statements of fact." Thus, it may not be a violation of the Rules to exaggerate or misstate in a negotiation "[e]stimates of price or value placed on the subject of a transaction and a party's intentions as to an acceptable settlement." *See* New York State Opinion 1228 (2021) ("'[A] party's intentions as to an acceptable settlement of a claim' will ordinarily not be taken as a statement of fact subject to the rule against false statements…[n]or will 'statements regarding … willingness to compromise.'"); *Otto v. Hearst Commc'ns, Inc.*, No. 17-CV-4712 (GHW) (JLC), 2019 WL 1034116, at *11 (S.D.N.Y. Feb. 21, 2019) ("It is not unusual in a negotiation for a party, directly or through counsel, to make a statement in the course of communicating its position that is less than entirely forthcoming.") (quoting ABA Formal Op. 06-439 (2006)) (alteration in original). Thus, in negotiating with a cyber-extortionist, as in negotiating with others in a more traditional setting, a lawyer may engage

[22] For example, the only rule that expressly requires a lawyer to abide by instructions of a client to take certain actions is Rule 1.2(a), which requires lawyers to "abide by a client's decision whether to settle a matter" and to abide by certain decisions of the client in the context of criminal cases. That rule is not implicated in the context of paying a ransom demanded of the lawyer or law firm by a cyber attacker. Rule 1.6(c) requires that a lawyer take reasonable care to prevent those working with the lawyer from disclosing confidential information. This requirement does not imply that a lawyer must pay a ransom to prevent disclosure of client confidential information.

[23] For a thorough analysis of the current ethical issues in the use of undercover investigators by lawyers, see NYCBA Professional Responsibility Committee & Ethics Committee, Proposed Amendment to Rule of Professional Conduct 8.4 Regulating Lawyers' Supervision of Undercover Investigators (Updated and Reissued December 2019) https://www.nycbar.org/reports/regulating-lawyers-supervision-of-undercover-investigations-report/?back=1.

[24] As the preamble to the Rules states, "[t]he Rules of Professional Conduct are rules of reason. They should be interpreted with reference to the purposes of legal representation and of the law itself." Preamble to the Rules, paragraph [6].

in the bluffing or puffery generally accepted in negotiations. For example, the Rules would not prohibit a lawyer from telling the cyber-extortionist that it is not acceptable to the lawyer to pay more than $100,000 in ransom, when that lawyer is willing to pay up to $200,000 if necessary to restore access to systems or recover confidential information.

But what if the lawyer were to make specific misrepresentations to the cyber-extortionist beyond negotiation bluffing, such as telling the cyber-extortionist that the lawyer has not reported the matter to the Federal Bureau of Investigation when the lawyer has in fact done so, or untruthfully responding to questions from the cyber-extortionist about the availability of cyber insurance coverage? The Committee believes that "generally accepted conventions" in negotiating with a cyber-extortionist to regain access to systems or recover confidential data are notably different than those for negotiating a settlement of a civil matter or negotiating terms of a transaction in the traditional setting and permit the lawyer or law firm to be not candid on facts relating to the impact of the cyber attack, the victim's financial situation, and any actions taken to mitigate the damage caused by the attack. Accordingly, while convention and supporting precedent require a lawyer to fully disclose insurance coverages in negotiating the settlement of a civil litigation, the same is not true in the context of responding to a cyber attack, where public policy and societal good are best served by thwarting the success of cyber-extortionists. The same is true for being less than transparent with cyber-extortionists about any steps the victim or its legal counsel or agents[25] have taken to respond to and mitigate the damage caused by the cyber attack, whether communicating with law enforcement or any other efforts.

New York City Opinion 2003-02 addresses an analogous situation relating to the undisclosed recording of conversations with others such as those "who have made threats against the attorney or client" or in the context of "the investigation of ongoing criminal conduct or other significant misconduct." This Committee opined that, while the undisclosed recording of conversations with others "smacks of trickery" and a lawyer engaging in such conduct would generally be in violation of Rule 8.4(c)'s predecessor, an undisclosed recording by a lawyer is ethically permitted in these types of limited situations where a "lawyer has a reasonable basis for believing that disclosure of the taping would significantly impair pursuit of a generally acceptable societal good."[26]

---

[25] Negotiating with cyber-extortionists has become a specialized field; many victims turn to specialized negotiators to instruct them on negotiations or to conduct the negotiations with cyber-extortionists on their behalf. These expert negotiators often work hand-in-hand with breach counsel and law enforcement in responding to the cybersecurity incident.

[26] Several other ethics opinions analyzing Rules 4.1 and 8.4(c) have found that the use of deception directed by attorneys, even in the course of representing a client, may be ethically permissible where the conduct is in the pursuit of a legitimate public interest. Although it has been the subject of criticism, New York County Opinion 737 (2007) found that in "certain exceptional conditions," such as when an attorney is investigating a violation of civil rights or intellectual property rights, "dissemblance by a non-attorney investigator supervised by an attorney is ethically permissible." But there are other ethics opinions that have reached similar conclusions. *See* 2014 North Carolina Opinion 9 (2015) (lawyer may "supervise the use of misrepresentation" in "the pursuit of a legitimate public interest" such as "investigations of discrimination in housing, employment and accommodations"); Arizona Opinion 99-11 (1999) ("lawyer ethically may direct a private investigator or tester to misrepresent their identity or purpose in contacting someone who is the subject of investigation, only if the misrepresentations are for the purpose of gathering facts before filing suit"). This Committee is also not aware of any lawyer who has been sanctioned for using deception that is not illegal with the perpetrator of a crime or directing others to do so where the lawyer is a victim.

Thwarting the success of cyber criminals is unquestionably in the interest of the public and societal good in general, as is protecting confidential information that clients entrust to their lawyers for the purposes of seeking legal advice. Indeed, to suggest that a lawyer and those acting at the lawyer's direction must be entirely forthright with a cyber-extortionist in negotiation would arguably weaken the public's trust in the legal profession rather than strengthen it, which is a primary purpose of Rule 4.1 and Rule 8.4(c). If clients knew that lawyers would be handcuffed by the Rules from following the generally accepted conventions of negotiating with cyber-extortionists to regain access to systems or to recover (or prevent further dissemination of) confidential data, clients may be less likely to provide lawyers with the information necessary to provide competent legal advice on sensitive matters.

While this Committee believes that it would be helpful to have clarifying amendments or additional commentary to the Rules, we do not believe that such clarifications are required to reach our conclusion here.

VI. Ethical Issues in Disclosing a Cybersecurity Incident to Law Enforcement or Cooperating in a Governmental Investigation

When a lawyer unintentionally loses control over confidential information, the lawyer may be obligated under Rules 1.1 and 1.6 to attempt to recover such information and prevent the further disclosure of confidential information, so long as such efforts are reasonable in the circumstances. For example, if a lawyer on the way to the airport accidentally leaves a box containing confidential client information in a taxi, the lawyer must make reasonable efforts to track down the taxi and recover the confidential information. Similarly, if while going through U.S. Customs, a lawyer's electronic device containing confidential information is seized for inspection, the attorney must "undertake[] reasonable efforts to dissuade border agents from reviewing clients' confidential information or to persuade them to limit the extent of their review." New York City Opinion 2017-5.

Similarly, we believe a lawyer or law firm that is a victim of a cybersecurity incident that compromises a client's material confidential information must take steps, if any are reasonably available, to prevent cyber criminals from using or further disclosing stolen client confidential information. However, as noted above, we do not believe that paying a ransom is necessarily an ethically required step in these circumstances. Nor, as discussed more fully below, is a lawyer or law firm under an ethical duty to report such incidents to law enforcement, who might be able to assist in recovering the stolen information. Indeed, as discussed below, reporting a cybersecurity incident may subject the law firm's clients to governmental scrutiny.

A lawyer or law firm that is the victim of a cybersecurity incident may want to report the incident to law enforcement or cooperate in a governmental investigation into the incident. For example, in some cases, law enforcement may be able to assist with stopping an ongoing cybersecurity incident or recovering client confidential information. In addition, a 2021 guidance from OFAC[27] states that a victim organization's prompt notification to and cooperation with law enforcement would be considered a mitigating factor in any potential sanctions risk the victim could face if it chooses to pay the ransom and the threat actor was later determined to be associated

[27] *Supra* fn. 20.

with a sanctioned entity. By reporting the incident or cooperating with a governmental investigation, the law firm may be assisting the government in preventing future attacks, thus acting as a good "corporate citizen."

In doing so, however, lawyers should be cognizant of their continuing confidentiality obligations to any current, former, or prospective clients who may have been impacted by the cybersecurity incident under Rules 1.6, 1.9, and 1.18. As stated in Rule 1.6:

> "Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential.[28]

Thus, the mere fact that a person or entity is or was a client may be confidential information. *See* New York State Opinion 1088 (2016). The fact that a client's confidential information was compromised in a cybersecurity incident is even more likely to be confidential under Rule 1.6.

If a lawyer does not obtain a client's consent to disclose its confidential information (which may be particularly difficult in the fast-moving scenario of a cybersecurity incident), a lawyer may disclose such information where "the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community." Rule 1.6(a)(2). This exception has been recognized as appropriate in situations where "time is of the essence and it is impractical for the lawyer to wait for the client's informed consent." New York State Opinion 991 (2013).

Thus, if a lawyer does not have time to get a client's consent, a lawyer may disclose a client's confidential information to law enforcement if the lawyer determines that disclosing the confidential information is (i) in the best interest of the *client* (*e.g.*, by stopping an ongoing breach or recovering a client's confidential information) and (ii) is reasonable under the circumstances.[29] However, in determining whether consent is impliedly authorized in these circumstances, we agree with ABA Formal Op. 483 that a lawyer should consider "whether the client would object to the disclosure [and] whether the client would be harmed by the disclosure." Furthermore, in disclosing confidential information, "the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information." ABA Formal Op. 483.

Lawyers should be aware that disclosing a client's identity as a victim of a cybersecurity incident could expose the client to potential liability. For example, in July 2023, the law firm Covington & Burling LLP was ordered to disclose to the Securities and Exchange Commission the identities of seven of the nearly 300 of its clients whose information was stolen. All seven were public company clients whose files had been compromised in a cybersecurity incident affecting

[28] "'Confidential information' does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates." Rule 1.6(a).

[29] The Committee is of the view that it is not "customary in the professional community" to disclose a client's confidential information to law enforcement in this context.

Covington and about which Covington had non-public information that was material to a potential buyer or seller of the client's securities. *SEC v. Covington & Burling, LLP*, No. 23-mc-00002 (APM), 2023 WL 4706125 (D.D.C. July 24, 2023). The SEC was seeking the identity of the clients "to determine . . . whether any [of Covington's clients] failed to make disclosures relating to the cyberattack." *Id*. at *1.

VII. Conflicts of Interest When the Lawyer's and Client's Interests Differ in Connection with the Cybersecurity Incident

Rule 1.7(a)(2) prohibits a lawyer from representing a client where a reasonable lawyer would conclude that:

> there is a significant risk that the lawyer's professional judgment on behalf of a client will be adversely affected by the lawyer's own financial, business, property or other personal interests.

While each cybersecurity incident is different, we think that such a conflict between a lawyer's personal interests and those of the client can sometimes arise.

For example, suppose that after notifying a client that the client's confidential information has been compromised in a cybersecurity incident, the client asks the lawyer to advise it with respect to its statutory notification obligations. However, the lawyer does not want the client to provide any notifications as it is not publicly known that the lawyer was the victim of a cybersecurity incident, and the lawyer believes it will suffer reputational risk and some of the lawyer's clients will cease working with the lawyer if they learn of this. We think in such situations, if the lawyer were to advise the client about the client's notification requirements, the lawyer most likely would have a conflict under Rule 1.7(a)(2)[30] and could only advise the client if (1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to the client in the matter and (2) the lawyer obtained informed consent from the client to the conflict, confirmed in writing. Rule 1.7(b)(1) and (4).

Consider another example. In investigating the cybersecurity incident, it may become clear that the lawyer failed to use "reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to" a client's confidential information as required by Rule 1.6(c) and may be subject to a malpractice claim by the client for the failure to use reasonable care.[31] In such a situation, under Rule 1.4, the lawyer has an obligation to notify the client of the "significant error or omission by the lawyer in his or her rendition of legal services." New York State Opinion 1092 (2016); New York State Opinion 734 (2000) (law firm "has an obligation to report to the client that it has made a significant error or omission that may give rise to a possible malpractice claim"). It is also possible that in such a situation the lawyer's continued representation of the client may be adversely affected by the lawyer's desire to avoid liability to the client, and

[30] If the lawyer merely has a preference not to make disclosure, this is unlikely to create a conflict.

[31] The failure to comply with a Rule of Professional Conduct is not in and of itself the basis for a civil claim. Preamble to the Rules, paragraph [12].

thus the lawyer would have a conflict under Rule 1.7(a)(2). *See* New York State Opinion 734; New York City Opinion 1995-2.

Conclusion

In the event of a cybersecurity incident, lawyers have ethical obligations to take appropriate steps to protect clients' confidential information (Section I). While lawyers and law firms may have statutory and regulatory notification requirements to which they are subject, they also have an ethical obligation under Rule 1.4 to promptly notify current clients in certain circumstances of the compromise of the confidentiality or availability of client information or if the law firm will likely be unable to meet material obligations to the client (Section II). There is no ethical prohibition against, or requirement to, pay a ransom to a cyber extortionist (Section IV) and lawyers and law firms may be not candid with respect to certain material facts when negotiating with cyber-extortionists in efforts to protect or regain access to client information and firm systems (Section V). Lawyers and law firms can only disclose client confidential information to law enforcement or in connection with a government investigation of a cybersecurity event if permitted by Rules 1.6, 1.9 or 1.18 and should be cognizant of potential risks to their clients of communicating with law enforcement or other government officials (Section VI). Finally, conflicts of interests may require the lawyer or law firm not to advise a client in connection with the cybersecurity incident or to cease representing the client altogether in the event of a malpractice claim arising from the incident (Section VII).