

CLE: Cyber Matters

April 18, 2024

Part 2: Mike Hoeflich

Resident Evil:

1. Malware that Keeps on Giving: Volt Typhoon and the Coming Cyber Apocalypse
2. Defending Against Resident Malware under the *Rules of Professional Responsibility*
3. Costs of data breaches, insurance, active monitoring

—Excerpted from **ABA Formal Opinion 477R** online at <https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/>:

The opinion takes a fresh look at advances in technology and ever-increasing cybersecurity threats, and provides guidance as to when enhanced security measures are appropriate.

This opinion is an update to ABA Formal Opinion 99-413 *Protecting the Confidentiality of Unencrypted E-Mail* (1999).

In 99-413, the committee concluded that since email provided a reasonable expectation of privacy, lawyers could use it to communicate with their clients, since it would be just as illegal to wiretap a telephone as it would be to intercept an email transmission. At the same time, the

committee recognized that some information is so sensitive that a lawyer might consider using particularly strong protective measures depending on the sensitivity of the information:

... The conclusions reached in this opinion do not, however, diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure and the relative security of the contemplated medium of communication. Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of email, just as they would warrant the avoidance of the telephone, fax and mail. – Formal Opinion 99-413 at page 2.

Since the time of Opinion 99-413, times have changed especially in the realm of technology and its many new and evolving manifestations that have become widespread in the profession. Laptop computers, smartphones, social media, cloud storage and Wi-Fi connections have become prevalent and much more commonplace than they were when 99-413 was written nearly 18 years ago.

...

1. Understand the nature of the threat. Consider the sensitivity of the client's information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted.

2. Understand how client confidential information is transmitted and where it is stored. Have a basic understanding of how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance.

3. Understand and use reasonable electronic security measures. Have an understanding of the security measures that are available to provide reasonable protections for client data. What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.

4. Determine how electronic communications about clients' matters should be protected. Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards such as encryption or password protection for attachments. Take into account the client's level of sophistication with electronic communications. If the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.

5. Label client confidential information. Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule [4.4\(b\)](#) *Respect for Rights of Third Persons*, the inadvertent recipient would be on notice to promptly notify the sender.

6. Train lawyers and nonlawyer assistants in technology and information security. Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures.

7. Conduct due diligence on vendors providing communication technology. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.

Excerpted from ABA Formal Opinion 483:

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-op-483.pdf

Formal Opinion 483 October 17, 2018

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction¹

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly

sensitive information, law firms are inviting targets for hackers.²

In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.³ Indeed, the data security threat is so high that law

enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.⁴ In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.⁵ This

1 This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

2 *See, e.g.,* Dan Steiner, *Hackers Are Aggressively Targeting Law Firms’ Data* (Aug. 3, 2017), <https://www.cio.com> (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); *See also Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

3 Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), <https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504>.

4 Robert S. Mueller, III, *Combating Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>.

5 ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Securing Communication of Protected Client Information”).

Formal Opinion 483

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,⁶ and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.⁷

⁶ The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other

organization.” How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer’s position in the firm. *See* MODEL RULES OF PROF’L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF’L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF’L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

7 In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.”) *See also, e.g., Cybersecurity Resources*, ABA Task Force on Cybersecurity, <https://www.americanbar.org/groups/cybersecurity/resources.html> (last visited Oct. 5, 2018).

Formal Opinion 483

I. Analysis

A. Duty of Competence

...Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to ‘keep abreast of changes in the law and its practice.’ The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing

competent legal services in today's environment without knowing how to use email or create an electronic document.

Formal Opinion 483

_____ 4

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.¹¹

1. Obligation to Monitor for a Data Breach

...Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

11 MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS

PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

Formal Opinion 483

____ _ 5

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that “such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.”

Applying this reasoning, and based on lawyers’ obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data¹² and the use of data. Without such a requirement, a lawyer’s recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,¹³ whether further action is warranted,¹⁴ whether employees are adhering to the law firm’s cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,¹⁵ and how and when the lawyer must take further action under other regulatory and legal provisions.¹⁶ Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.¹⁷

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not

necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

Formal Opinion 483

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

...The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

Formal Opinion 483

define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a

competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."²¹ These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances...

.

...

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.²³ The 2012 modification added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."²⁴

Amended Comment [18] explains:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or

unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors 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, and

Formal Opinion 483

- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).²⁵

As this Committee recognized in ABA Formal Opinion 477R:

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or

impenetrable.²⁶ Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access. As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

Although security is relative, a legal standard for “reasonable” security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a “process” to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.

Formal Opinion 483

...

C. Lawyer’s Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.³⁰ We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must “keep the client reasonably informed about the status of the matter.” Rule 1.4(b) provides: “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.” Under these provisions, an obligation

exists for a lawyer to communicate with current clients about a data breach.

Formal Opinion 483

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a “serious breach.”³² The Committee advised:

Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).

A data breach under this opinion involves the 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 by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a “client reasonably informed about the status of the matter” and the lawyer should provide information as would be “reasonably necessary to permit the client to make informed decisions regarding the representation” within the meaning of Model Rule 1.4.34

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients...

Formal Opinion 483

Model Rule 1.15(a) provides that a lawyer shall hold “property” of clients “in connection with a representation separate from the lawyer’s own property.” Funds must be kept in a separate account, and “[o]ther property shall be identified as such and appropriately safeguarded.” Model Rule 1.15(a) also provides that, “Complete records of such account funds and other property shall be kept by the lawyer”

Comment [1] to Model Rule 1.15 states:

A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property.

An open question exists whether Model Rule 1.15’s reference to “property” includes information stored in electronic form. Comment [1] uses as examples “securities” and “property” that should be kept separate from the lawyer’s “business and personal property.” That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15’s safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, “Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information.” The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

Formal Opinion 483

13 2. Former Client

Model Rule 1.9(c) requires that “A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client.”³⁵

When electronic “information relating to the representation” of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer’s obligation to notify the former client. Rule 1.9(c) provides that a lawyer “shall not . . . reveal” the former client’s information. It does not describe what steps, if any, a lawyer should take if such information is revealed. 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.³⁶

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.³⁷ We also note that Rule 1.16(d) directs that lawyers should return “papers and property” to clients at the conclusion of the representation, which has commonly been understood to include the client’s file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.³⁸ Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client’s electronic information that is in the lawyer’s possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

Formal Opinion 483

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients...

reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything.

In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access

or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact. In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

39 Cf. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

Formal Opinion 483

information. Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.⁴¹ Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.⁴² Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.⁴³ Many federal and state agencies also have confidentiality and breach notification requirements.⁴⁴ These regulatory schemes have the potential to cover individuals who meet

particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.⁴⁵

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

END