




ABA Formal Opinion 483: Attorneys' Obligations Relating to Cyberattacks


By Joshua Bevitz

1

Presenter Information



Joshua Bevitz
Joshua.Bevitz@ndlf.com
925.988.3226



© 2021 Newmeyer & Dillion LLP. All Rights Reserved | newmeyerdillion.com

2

Ensure Reasonable Computer Protection Systems Are In Place

- Model Rule 1.1 and Comment 8 to Rule 1.1.
- Every law firm should have current technology protection.
- Every law firm should perform periodic, regular reviews to determine whether additional protections are warranted and whether the current security system in place is “reasonable.”

© 2021 Newmeyer & Dillion LLP. All Rights Reserved | newmeyerdillion.com



3

Ensure Reasonable Computer Protection Systems Are In Place

- Every law firm should monitor whether patching existing protections is necessary based on newly developed cyberattacks.
- At least one technically-competent partner should be assigned as the liaison to the IT Department to ensure its responsibilities are being met. If a law firm does not have an IT Department, an outside cybersecurity firm should be consulted and retained.

© 2021 Newmeyer & Dillion LLP. All Rights Reserved | newmeyerdillion.com



4

Train and Test Your Attorneys and Staff

- Most successful cyberattacks are the result of human error.
- All users should be regularly trained regarding what types of cyberattacks, and what attackers try to do to trick users.
- Law firms should take matters a step further and conduct fake phishing campaigns to test their employees.
- Numerous third-party cyber companies can provide this service if a firm does not have internal resources to do so.

© 2021 Newmeyer & Dillion LLP. All Rights Reserved | newmeyerdillion.com



5

Ensure Third Party Vendors Have Reasonable Cyber Protection Systems in Place

- Law firms should ensure that external vendors have reasonable security protections in place.
- If a vendor does not have reasonable protections, the vendor must be required to implement such protections immediately.
- One proven approach for law firms is to contractually require vendors to adhere to a specific cybersecurity framework and to provide the law firm the right to audit them.

© 2021 Newmeyer & Dillion LLP. All Rights Reserved | newmeyerdillion.com



6

Limit The Amount Of Time Client Files Are Retained

- The longer a law firm retains its electronic files, the longer those files are susceptible to being attacked.
- Every law firm should have a written document retention policy.
- The amount of time client files are retained after the conclusion of a matter should be limited as agreed to as part of the initial engagement agreement.

© 2021 Newmeyer & Dillon LLP. All Rights Reserved | newmeyerdillon.com



7

Know How to Respond

- Law firms should have a plan in place to deal with cyberattacks when they happen.
- One of the key steps in the response plan should include discovering what occurred and whether client data was compromised.
- The notification should be sufficiently detailed so that the client can decide what next steps, if any, should be taken as a result of the attack.

© 2021 Newmeyer & Dillon LLP. All Rights Reserved | newmeyerdillon.com



8

Know How to Respond

- Law firms should also make sure they notify clients of any efforts to recover data and what additional protections, if any, are being put into place.
- Failing to take the steps outlined above could not only result in the breach of an attorney's ethical duties, but it could also lead to civil liability.

© 2021 Newmeyer & Dillion LLP. All Rights Reserved | newmeyerdillion.com

**NEWMAYER
DILLION** 

9

Thank You!

About Newmeyer Dillion

Growing and thriving businesses throughout California and Nevada trust us for advice that propels them to success. From advising on best practices to keep your information safe, to mitigating risk when a breach occurs, we help companies in diverse industries prepare for what's ahead.

**NEWMAYER
DILLION** 

10



CYBER LIABILITY

Presented by Chantal Rees
Rees & Rees Insurance Services
925-464-7811
reesandreesinsurance@gmail.com



1

What Does Cyber Liability Cover?

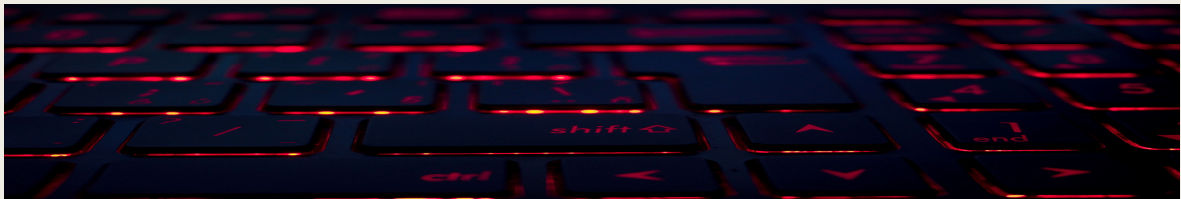
- **Privacy Liability:** Covers the cost associated with a breach for court defense costs and indemnity.
- **Regulatory:** Covers fines and penalties from state and federal agencies including HIPAA.
- **Security Breach Response:** Dollars for the IT Forensics, Lawyers, Notifications, PR firm, Credit Monitoring, Call Centers, etc. This is the coverage that notifies your clients of a breach, secures your network, and notifies the attorney general in all states you do business. This is the triage center for a claim.
- **Security Liability:** Suits and costs that arise due to a distribution of malicious code to others via your systems.



2

What Does Cyber Liability Cover?

- **Business Interruption / Data Restoration:** If the network has been damaged and it is down for an extended period of time, insureds can recoup the funds they would have earned during the time they were down. Data restoration is restores the information that was damaged or deleted during a breach. The first question on the application asks if data backups are completed once a week. If the insured does not back up their data once a week, then they do not receive this insuring agreement.



3

What Does Cyber Liability Cover?

- **Media Liability:** This coverage applies to your website and print material for copy write material, libel, slander, and if someone were to hack your site and add malicious information.

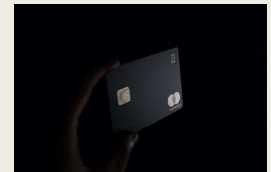
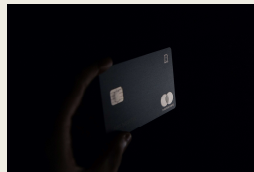


- **Extortion:** This is for if a hacker were to request funds either to stop a disruption or prevent a disruption in your network. Example 1 – your network is locked and they request funds to give you the password to unlock your network. Example 2 – hacker tells you they will launch a DDOS attack (denial of services attack) if your do not pay bitcoin. (DDOS attack will overload your network with information and then the network will go down).

4

What Does Cyber Liability Cover?

- **PCI Assessments (Payment Card Industry):** The PCI fines and assessments are assessed if the insured is not in compliance with the PCI rules of accepting cards, or there is a breach of card information. The PCI will typically make the insured aware that they need to amend their practices, and if they don't they will start getting fines/penalties.



5

What Does Cyber Liability Cover?



- **Cyber Deception (if elected):** The coverage provides reimbursement for release of funds due to deceptive instructions to release a wire transfer to a fraudulent bank account. Example – Accounting department receives an email that looks like it is coming from the President of the organization. The email is requesting an invoice be paid, and provides a wire transfer number. The accounting department releases the funds, but soon after it is discovered the email was fraudulent. The policy can reimburse the insured if the dual controls for releasing funds were properly followed.

6

What is Needed to Obtain Coverage?

- All quotes are based on gross sales.
- Past claims will affect premiums and/or offers of coverage.
- Most quotes available in minutes, however, some industries require further review (technology, cannabis, debt collecting, etc.)
- Required before binding:
 - Backups must occur weekly to an offsite location.
 - Antivirus and firewalls must be in place and updated regularly.
 - Dual control when transferring funds in excess of \$10,000 to external parties.

7

What is the Typical Cost of a Policy?

1. For Legal Services making about \$1M a year, the price can range from \$1,492 to \$3,690 depending on the product selection.
2. A domestic services contractor making \$5M per year in revenue would be anywhere from \$1,496 up to \$2,910.
3. A consulting firm with a contract requirement of \$5M of cyber liability coverage would come in about \$13,880.
4. Small start up IT firm estimating about \$90K in gross revenue would pay about \$2,255 for cyber liability and professional liability combined.



8



9

Small Breach: 1,000 Records

INCIDENT INVESTIGATION

FORENSICS INVESTIGATION	\$31,500	<input type="radio"/>
SECURITY REMEDIATION	\$101,000	<input type="radio"/>
BREACH COACH & LEGAL GUIDANCE	\$38,000	<input type="radio"/>
SUBTOTAL	\$170,500	

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

CUSTOMER NOTIFICATION	\$15,000	<input type="radio"/>
CALL CENTER	\$375	<input type="radio"/>
CREDIT/ID MONITORING	\$18,750	<input type="radio"/>
PUBLIC RELATIONS	\$36,000	<input type="radio"/>
SUBTOTAL	\$70,125	

CLASS ACTION LAWSUIT

DEFENSE	\$367,900	<input type="radio"/>
eDISCOVERY	\$126,000	<input type="radio"/>
SETTLEMENT/DAMAGES	\$150,000	<input type="radio"/>
SUBTOTAL	\$643,900	

PCI

FINES & PENALTIES	\$0	<input type="radio"/>
FRAUD ASSESSMENTS	\$0	<input type="radio"/>
CARD REISSUANCE	\$0	<input type="radio"/>
SUBTOTAL	\$0	

REGULATORY FINES & PENALTIES

STATE AG	\$6,650	<input type="radio"/>
HHS	\$0	<input type="radio"/>
OTHER (FTC, SEC, ETC.)	\$101,250	<input type="radio"/>
SUBTOTAL	\$107,900	

TOTAL COST \$992,425

PER RECORD COST \$198

10

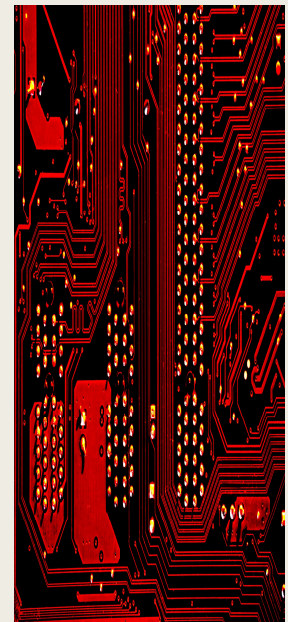
Common Misconceptions

- I have coverage on my general liability policy.
- My IT firm handles these issues for me. *It's a partnership.
- I don't keep anything on my network, it is all stored in the cloud or I don't keep any sensitive information on my computer.
- I am a small company, no one will want my data.
- We only keep paper files so data breach is not possible.

11

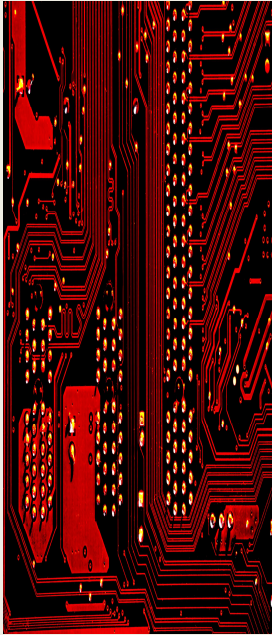
- In 2013, the Target data breach was caused by an HVAC contractor who had network credentials for Target's system for billing purposes.
- In May 2020, hackers targeted a high-profile law firm in New York with multiple A-list celebrity clients. They demanded an undisclosed sum of money to avoid releasing sensitive data about the clients. Here is the link to the article: <https://www.bbc.com/news/technology-52632729#:~:text=A%20law%20firm%20used%20by,including%20contracts%20and%20personal%20emails>
- University of California, San Francisco paid hackers over \$1M after information was held for ransom. Read the full story here: <https://www.bbc.com/news/technology-53214783>

Examples



12

Examples



- One of our clients had an email come from the “owner” requesting \$25,000 in gift cards be purchased and mailed out to various addresses. The employee completed the task and discovered after the fact that it was a fake email. Merchant services would not reimburse the company because an employee had made the purchases.
- Whiting-Turner, an accounting firm, was breached in 2016 and their clients’ W-2 and 1095 tax forms were exposed. Fraudulent taxes were filed in employees’ names and children of employees who received healthcare benefits had names, DOB and SS numbers exposed.

13



THANK YOU!

Chantal Rees

Rees & Rees Insurance Services

925-464-7811

reesandreesinsurance@gmail.com



14

The Canary in the Coal Mine

Am I Secure?

Answering the most difficult question in IT Support.

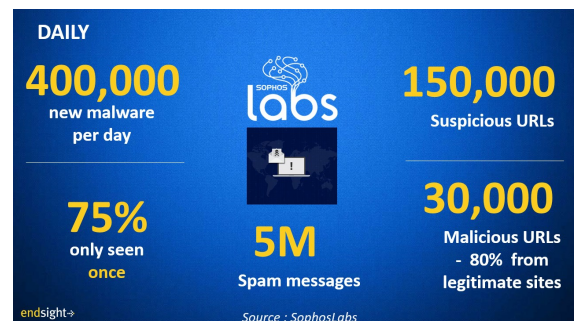
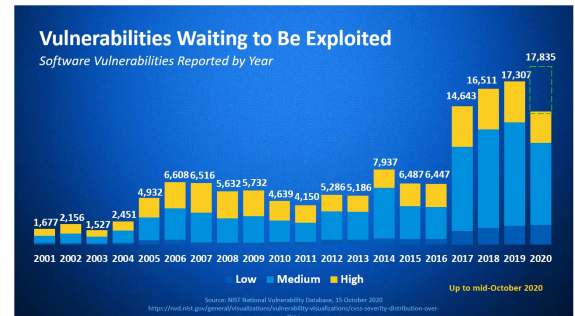
The number one question I get as an Outsourced IT Provider is "am I secure?" This question is difficult to answer because I am on the outside looking in. I am not your IT Provider. Can't I just provide a security audit? Yes, but it won't help you actually be any more secure. An audit will simply cost you thousands of dollars, and bring to the forefront the problems your IT resource either (1) didn't know were problems, or (2) have been ignoring because they can't fix them. Even then, an audit will give you a sense of your security concerns today... but what about tomorrow, or a week from now?

The world of security is changing in real-time, faster than you can imagine. Security is not just about best practice anymore, response matters too. Your IT resource must be as nimble as the bad actors. A list of IT vulnerabilities from weeks ago when an audit was completed will not make you secure.

Instead, organizations like the Center for Internet Security have published helpful guidelines for security professionals to follow. Authorities like the California Attorney General have pointed at the CIS 18 as a reasonable standard for security. Yet again though, these are highly technical and difficult for many business leaders to properly chaperon.

The following questions have been developed to serve as a canary in the coal mine. These questions are a test to see if an IT environment might be compliant with the 18 controls.

The goal is NOT to ask the IT resource to start doing these things. We are simply testing to see if there is evidence that the much harder to complete (and assess) work has been done already. The things these questions ask for are a reasonable outcome of properly deployed controls.



#1 Top Safeguard to ask about each the Top 3 CIS Controls

1 Inventory & control of enterprise assets*

At this moment, can you produce a complete list of every enterprise asset* physical as well as non-physical (virtual, remote, cloud environments) or anything else regularly connected to the enterprise network infrastructure? Is it updated bi-annually?

2 Inventory & Control of Software Assets

At this moment, can you produce an accurate list of every software in use at the company, including the number of licenses with recurring fees or one-time purchase?

3 Data Protection

Can you show me a written data management process for handling data with details such as data sensitivity, data owner, data retention limits, and data disposal requirements that is updated annually?

*enterprise assets – hardware and devices: all computers, servers, network devices, accessories including end-user devices such as mobile phones, non-computing devices, Internet of Things devices.

If you get a NO to any of these questions, the result should not be to undertake a project to turn them into a YES. These are leading indicators that something essential to security is not being done. I cannot say that you are definitely secure, but you pass the first test. If the answer to any of these is NO, then I can say that it's time for swift and dramatic action to address cyber security.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

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's 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, *Combatting 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").

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).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”⁸ The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)⁹

In recommending the change to Rule 1.1’s Comment, the ABA Commission on Ethics 20/20 explained:

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.¹⁰

⁸ MODEL RULES OF PROF’L CONDUCT R. 1.1 (2018).

⁹ A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

¹⁰ ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_a_mended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer’s substantive duty of competence: “Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase ‘including the benefits and risks associated with relevant technology,’ would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general ethical duty to remain competent.”

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

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

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].

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

¹² ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 08-451 (2008).

¹³ Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), available at <https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx> (noting that “[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization’s IT environment.”).

¹⁴ MODEL RULES OF PROF’L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF’L CONDUCT R. 1.15 (2018).

¹⁵ See also MODEL RULES OF PROF’L CONDUCT R. 5.1 & 5.3 (2018).

¹⁶ The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, <https://www.us-cert.gov/ais> (last visited Oct. 5, 2018); See also National Cyber Security Centre “Ten Steps to Cyber Security” [Step 8: Monitoring] (Aug. 9, 2016), <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

¹⁷ ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017).

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

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.¹⁸ The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. “One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents.”¹⁹ While every lawyer’s response plan should be tailored to the lawyer’s or the law firm’s specific practice, as a general matter incident response plans share common features:

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

¹⁸ See ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting “an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.”).

¹⁹ NIST Computer Security Incident Handling Guide, at 6 (2012), <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.

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.²⁰

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.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

²⁰ Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

²¹ We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).²² Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

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

²² The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

²³ MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

²⁴ *Id.* at (c).

- 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.²⁷ 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.²⁸

²⁵ MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. [18] (2018). “The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available.” ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

²⁶ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

²⁷ MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. [18] (2018) (“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.”)

²⁸ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.²⁹ In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

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.³¹

²⁹ ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

³⁰ This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

³¹ Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: “If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

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).³³

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. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients “reasonably informed about the status” of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.”) (*citations omitted*).

³² ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

³³ *Id.*

³⁴ MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

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.

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

³⁵ MODEL RULES OF PROF’L CONDUCT R. 1.9(c)(2) (2018).

³⁶ See *Discipline of Feland*, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent’s argument that the court should engraft an additional element of proof in a disciplinary charge because “such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.”).

³⁷ See MODEL RULES OF PROF’L CONDUCT R. 1.9, cmt. [9] (2018).

³⁸ See ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

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.³⁹

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or 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).

information.⁴⁰ 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 breach, 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

⁴⁰ State Bar of Mich. Op. RI-09 (1991).

⁴¹ National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.

⁴⁵ Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

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.”

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

CHAIR: Barbara S. Gillers, New York, NY ■ John M. Barkett, Miami, FL ■ Wendy Wen Yun Chang, Los Angeles, CA ■ Hon. Daniel J. Crothers, Bismarck, ND ■ Keith R. Fisher, Arlington, VA ■ Douglas R. Richmond, Chicago, IL ■ Michael H. Rubin, Baton Rouge, LA ■ Lynda Shely, Scottsdale, AZ ■ Elizabeth C. Tarbert, Tallahassee, FL. ■ Allison Wood, Chicago, IL

CENTER FOR PROFESSIONAL RESPONSIBILITY: Dennis A. Rendleman, Ethics Counsel

©2018 by the American Bar Association. All rights reserved.