



NELA/NY Spring 2023 Conference

Fordham Law School

May 5, 2023

Cyber Security for Attorneys

Patrick DeLince, Esq.

Jason Rebholz

How to Stay Secure in a Digital World

- Legal Landscape
 - What are you required to know about Cyber Security
 - The cyber security treat to law firms
 - The competent lawyer
 - NYS CLE Requirements
- Current Cyber Threat Landscape
 - What are the security threats you face every day?
 - What does it mean to be “hacked?”
 - What is a data breach?
- Security Best Practices - How to Protect Yourself on a Budget
 - Account Security
 - Password management
 - Multi-factor authentication
 - Enhanced email protection and authentication
 - Online Security
 - Phishing awareness
 - Safe web browsing
 - Wireless security
 -
 - Endpoint security
 - Antivirus

- Data Security
 - Protecting your data
 - Securely transferring data
- Protecting your income
 - Cyber security insurance
 - Sources for more information on securing your data

Table of Contents

CLE - Cybersecurity-Privacy-and-Data-Protection-FAQs	2
Rule 1.6_ Confidentiality of Information	9
Securing communication of protected client information - ABA Formal Opinion 477R	10
Lawyers' Obligations After an Electronic Data Breach or Cyberattack - ABA_Formal_Opinion_483	13
NYSBA Ethics Opn: E-mailing documents that may contain hidden data reflecting client confidences and secrets	29
NYSBA Ethics Opn: Use of computer software to surreptitiously examine and trace e-mail and other electronic documents	32
Law Firms Are Under Attack	13
The Top 11 Legal Industry Cyber Attacks (March 29, 2022)	36
NYSAG - Data Security v. Heidell, Pittoni, Murphy & Bach LLP (March 3, 2023)	46
Security Incident March 2023 Update & Actions - LastPass	62
Protecting your income	67
Cybersecurity Insuranc_ Federal Trade Commission -	67
CYBER INSURANCE	67
WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?	67
WHAT IS FIRST-PARTY COVERAGE AND WHAT SHOULD YOU LOOK FOR?	68
WHAT IS Third-party coverage AND WHAT SHOULD YOU LOOK FOR?	68
Cybersecurity for Small Business _ Federal Trade Commission	69
The Panel	73
J. Patrick DeLince	73
Jason Rebholz Bio	74

Cybersecurity, Privacy and Data Protection FAQs

The following Frequently Asked Questions (FAQs) relate to the changes in the New York State CLE Program Rules and the New York State CLE Board Regulations and Guidelines adding Cybersecurity, Privacy and Data Protection as a new CLE category of credit (effective January 1, 2023) and requiring that attorneys complete at least 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of their biennial CLE requirement (effective July 1, 2023).

Experienced Attorney FAQs

Q] What is the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] Experienced attorneys (admitted to the New York Bar for more than two years) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their biennial CLE requirement. Attorneys may complete the requirement by taking Cybersecurity, Privacy and Data Protection-**General** or Cybersecurity, Privacy and Data Protection-**Ethics** programs, or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics**.

Q] Does the new Cybersecurity, Privacy and Data Protection requirement increase the total number of CLE credit hours that experienced attorneys must complete during each biennial reporting cycle?

A] No, experienced attorneys must still earn at least 24 CLE credit hours each biennial reporting cycle as follows:

Experienced Attorney Required CLE Categories (for attorneys due to re-register on or after July 1, 2023)	Required CLE Credit Hours
Ethics and Professionalism	4
Diversity, Inclusion and Elimination of Bias	1
Cybersecurity, Privacy and Data Protection (General or Ethics)	1*
Any CLE category of credit	18
Total Number of CLE credit hours	24

*You may choose to complete the Cybersecurity credit in Cybersecurity **General** or Cybersecurity **Ethics** (or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics**).

You may count a maximum of 3 credit hours of Cybersecurity **Ethics** -- but not Cybersecurity **General** -- toward your 4-credit Ethics and Professionalism requirement.

- *Example:* if you earn 3 credits in Cybersecurity Ethics, then you still need to earn 1 credit in Ethics and Professionalism, 1 credit in Diversity, Inclusion and Elimination of Bias and 19 credits in any category of credit -- total of 24 credits

Q] When can I start to earn CLE credit in the new Cybersecurity, Privacy and Data Protection category?

A] You may earn CLE credit in the Cybersecurity, Privacy and Data Protection category beginning on January 1, 2023.

Q] When must I begin to comply with the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] The new requirement becomes effective July 1, 2023.

- If you are **due to re-register on or after July 1, 2023 (birthday is on or after July 1st)**, you must complete 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of your biennial CLE requirement.
- If you are **due to re-register in 2023 but your birthday is before July 1st**, you need **not** comply with the new requirement in 2023, but must comply in future biennial periods.
 - Example: If your birthday is on June 30th and you are due to re-register in 2023, then you do not need to comply with the new requirement in 2023, even if you file your registration form on or after July 1, 2023.
- If you are due to re-register in 2024, or later, you must comply with the new requirement.

Q] I'm due to re-register on or after July 1, 2023, but I won't be able to complete the Cybersecurity, Privacy and Data Protection requirement on time. What should I do?

A] You may apply for an [extension of time](#) to complete the CLE requirement.

Q] If I took a cybersecurity course before January 1, 2023, can I apply the credit earned from that course towards my Cybersecurity, Privacy and Data Protection CLE requirement?

A] No, only CLE courses that you take from January 1, 2023 onwards may count towards the Cybersecurity, Privacy and Data Protection CLE requirement.

Q] May I satisfy any of my Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-Ethics courses?

A] Yes, you may satisfy a maximum of 3 credits of your Ethics and Professionalism requirement with the same number of Cybersecurity, Privacy and Data Protection-Ethics credits.

Q] May I carry over Cybersecurity, Privacy and Data Protection CLE credits from one biennial reporting cycle to the next?

A] Yes. Once you have completed the 24-CLE credit requirement, a maximum of 6 additional credits earned may be applied toward the next reporting cycle. Experienced attorneys may carry over credits in any category, including Cybersecurity, Privacy and Data Protection, from one cycle to the next.

Newly Admitted Attorney FAQs

Q] What is the new Cybersecurity, Privacy and Data Protection CLE requirement?

- A] Newly admitted attorneys (admitted to the New York Bar for two years or less) must complete at least 1 CLE credit hour in the Cybersecurity, Privacy and Data Protection CLE category of credit as part of their newly admitted cycle requirement. Attorneys may complete the requirement by taking Cybersecurity, Privacy and Data Protection-**General** or Cybersecurity, Privacy and Data Protection-**Ethics** programs, or a combination of the two: ½ credit in Cybersecurity **General** and ½ credit in Cybersecurity **Ethics**.

Q] Does the new Cybersecurity, Privacy and Data Protection requirement increase the total number of CLE credit hours that newly admitted attorneys must complete during the newly admitted cycle?

- A] No, newly admitted attorneys must still earn a total of 32 CLE credit hours (with 16 credit hours each year) in the newly admitted cycle as follows:

Newly Admitted Attorney Required CLE Categories (for attorneys admitted on or after July 1, 2023)	Year 1 CLE Credit Hours	Year 2 CLE Credit Hours
Law Practice Management, Areas of Professional Practice, and/or Cybersecurity, Privacy and Data Protection- General	7 see below	7 see below
Skills	6	6
Ethics and Professionalism	3	3
Cybersecurity, Privacy and Data Protection- Ethics	see below	see below
Total Number of CLE credit hours	16	16

Cybersecurity, Privacy and Data Protection (“Cybersecurity”) Category

- You must complete at least 1 credit in Cybersecurity as part of the 32-credit requirement.
- You may choose to complete the Cybersecurity credit:
 - in Year 1 or Year 2 (as part of the 16 credit-requirement for that year)
 - in Cybersecurity **General** or Cybersecurity **Ethics** (or a combination of the two)
- You may apply a maximum of 3 credit hours of Cybersecurity **Ethics** -- but not Cybersecurity **General** -- toward your 6-credit Ethics and Professionalism requirement
 - Example:* if you complete 1 credit in Cybersecurity **Ethics** in Year 1, you satisfy your Cybersecurity requirement, and then need to complete only 2 credits in Ethics and Professionalism for that year.
 - Example:* if you complete 1 credit in Cybersecurity **General** in Year 1, you satisfy your Cybersecurity requirement and must complete an additional 6 credits in Law Practice Management, Areas of Professional Practice, and/or Cybersecurity, Privacy and Data Protection-**General** for that year.

Q] When must I begin to comply with the new Cybersecurity, Privacy and Data Protection CLE requirement?

A] The new requirement becomes effective July 1, 2023 for attorneys **admitted to the NY Bar on or after July 1, 2023**.

- If you were admitted to the NY Bar **prior to July 1, 2023**, you need not comply with the Cybersecurity, Privacy and Data Protection requirement in your newly admitted cycle, but must comply in future reporting cycles.
- Attorneys admitted to the NY Bar **on or after July 1, 2023**, must complete 1 CLE credit hour in Cybersecurity, Privacy and Data Protection as part of their newly admitted attorney CLE requirement.

Q] When can I start to earn CLE credit in the new Cybersecurity, Privacy and Data Protection category?

A] You may earn CLE credit in the Cybersecurity, Privacy and Data Protection category beginning on January 1, 2023.

Q] If I took a cybersecurity course before January 1, 2023, can I apply the credit earned from that course towards my Cybersecurity, Privacy and Data Protection CLE requirement?

A] No, only CLE courses that you take from January 1, 2023 onwards may count towards the Cybersecurity, Privacy and Data Protection CLE requirement.

Q] Do I need to complete the Cybersecurity, Privacy and Data Protection CLE requirement in each year of my newly admitted cycle, i.e., 1 Cybersecurity CLE credit in Year 1 and 1 Cybersecurity CLE credit in Year 2?

A] No, you only need to complete 1 CLE credit in Cybersecurity, Privacy and Data Protection during your newly admitted cycle.

Q] Do I need to complete the 1-credit Cybersecurity, Privacy and Data Protection CLE requirement during the first or second year of my newly admitted cycle?

A] You can choose to complete the 1-credit Cybersecurity, Privacy and Data Protection CLE requirement in the first or second year of your newly admitted cycle as part of your 16-credit requirement for the year.

Q] May I carry over Cybersecurity, Privacy and Data Protection CLE credits?

A] Credit in Cybersecurity, Privacy and Data Protection-**Ethics** may not be carried over. Credit in Cybersecurity, Privacy and Data Protection-**General** may be carried over. For more information on carryover credit, please read the [Newly Admitted FAQs](#).

- Q] Do Cybersecurity, Privacy and Data Protection credits count toward my Ethics and Professionalism requirement?**
- A] You may count a maximum of 3 Cybersecurity, Privacy and Data Protection-**Ethics** credits toward your Ethics and Professionalism requirement in your newly admitted cycle. Cybersecurity, Privacy and Data Protection-**General** credits **do not** count toward your Ethics and Professionalism requirement.
- Q] May I satisfy my entire Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-Ethics courses?**
- A] No, you may satisfy a maximum of 3 credits of your total 6-credit Ethics and Professionalism requirement by completing Cybersecurity, Privacy and Data Protection-**Ethics** courses. By doing so, you would also satisfy your 1-credit Cybersecurity requirement.
- Q] As a newly admitted attorney, in what formats can I take Cybersecurity, Privacy and Data Protection courses?**
- A] For Cybersecurity, Privacy and Data Protection-**General** courses, you may earn CLE credit in **any** approved format, including on-demand audio/video or webconference. For Cybersecurity, Privacy and Data Protection-**Ethics** courses, you may earn CLE credit **only** in traditional live classroom, fully interactive videoconference, or in other live formats (e.g., webconferences, teleconferences) where questions are permitted during the course.

Provider FAQs

Q] What may be addressed in Cybersecurity, Privacy and Data Protection programs?

A] Cybersecurity, Privacy and Data Protection CLE programs must relate to the practice of law, be specifically tailored to a legal audience, and aim to increase attorneys' professional **legal** competency. Please read [Guidance for CLE Providers relating to Cybersecurity Ethics program areas and Cybersecurity General program areas](#).

Q] When may we begin to issue CLE credit in Cybersecurity, Privacy and Data Protection?

A] Providers may begin to issue credit in Cybersecurity, Privacy and Data Protection as of January 1, 2023, to attorneys who complete courses in this new category on or after January 1, 2023.

Q] What are the permissible formats for Cybersecurity, Privacy and Data Protection courses?

A] Experienced Attorneys: for Cybersecurity, Privacy and Data Protection (Ethics and General) courses, experienced attorneys may earn CLE credit in **any** approved format, including on-demand audio/video or webconference.

Newly Admitted Attorneys:

- for Cybersecurity **General** courses, newly admitted attorneys may earn CLE credit in **any** approved format, including on-demand audio/video or webconference.
- for Cybersecurity **Ethics** courses, newly admitted attorneys may earn CLE credit **only** in traditional live classroom, fully interactive videoconference, or in other live formats (e.g., webconferences, teleconferences) where questions are permitted during the course.

Q] We offered a live cybersecurity training in 2022 or earlier; can we issue CLE credit in the Cybersecurity, Privacy and Data Protection category to the attendees of this training?

A] No, you may not issue CLE credit in Cybersecurity, Privacy and Data Protection to the attendees of live courses that occurred prior to January 1, 2023.

Q] May we issue revised certificates awarding credit in the new Cybersecurity, Privacy and Data Protection category to attorneys who completed cybersecurity training in 2022 or earlier?

A] No. You may not issue revised certificates of attendance awarding credit in Cybersecurity, Privacy and Data Protection for courses completed prior to January 1, 2023.

Q] We issued CLE credit in Law Practice Management and Ethics and Professionalism for a course on cybersecurity in 2022 and we recorded the training. Can we issue CLE credit in the Cybersecurity, Privacy and Data Protection CLE category to participants who complete the prerecorded program on or after January 1, 2023?

A] Yes, assuming the content of the prerecorded program is timely and falls within the definition of Cybersecurity, Privacy and Data Protection, you can issue credit in Cybersecurity, Privacy and Data Protection to attorneys who complete the prerecorded program on or after January 1, 2023. Please note -- for newly admitted attorneys, the prerecorded format is permissible for credit in Cybersecurity, Privacy and Data Protection-**General** but not for credit in Cybersecurity, Privacy and Data Protection-**Ethics**.

Q] Can we issue CLE credit in Cybersecurity, Privacy and Data Protection training where there is no attorney faculty member participating?

A] No. As with all CLE programs, the faculty for a Cybersecurity, Privacy and Data Protection program should include an attorney in good standing who must actively participate in the program.

Q] Will there be a revised New York CLE Certificate of Attendance?

A] Yes, a revised New York CLE Certificate of Attendance that includes Cybersecurity, Privacy and Data Protection will be available on the CLE website and must be used beginning on January 1, 2023.

Rule 1.6: Confidentiality of Information

Client-Lawyer Relationship

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

(c) 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.

[Comment](#) | [Table of Contents](#) | [Next Rule](#)

ABA Formal Opinion 477R: Securing communication of protected client information

Just this past week, the [ABA Standing Committee on Ethics and Professional Responsibility](#) issued [Formal Opinion 477R](#) (Revised May 22, 2017) on the subject of a lawyer's ethical obligations to protect confidential client information when transmitting information relating to the representation over the internet. 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.

The [ABA Model Rules of Professional Conduct](#) have also undergone several changes, particularly those that focus on a lawyer's obligation to protect client confidences when transmitting information over the internet.

Chief among these were the amendments to [Rule 1.1](#) *Competence* and [1.6](#) *Confidentiality of Information* of the ABA Model Rules of Professional Conduct that were proposed by the [ABA Ethics 20/20 Commission](#) and subsequently adopted by the ABA House of Delegates at the 2012 ABA Annual Meeting. (The Ethics 20/20 Commission's Report and Recommendation concerning these amendments is available [here](#).)

Paragraph 8 of the Comment to Rule 1.1 now states that “a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks of technology...*”

The commission also added a new subpart (c) to Rule 1.6 that states:

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.

Paragraph 18 of the Comment to Rule 1.6 was also amended, making it clear that additional methods of security should be considered depending upon the sensitivity of the information that is to be transmitted.

In Opinion 477R, the committee took note of the increasing sophistication of cyber threats in today’s technological environment and recognized that some new forms of electronic communication that have become commonplace may not in every instance provide a reasonable expectation of privacy:

...In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable - Formal Opinion 477R at p. 5

In order to determine when additional security methods are required, the committee turned to the factors outlined in paragraph 18 of the Comment to Model Rule 1.6:

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

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).

The committee recommended the following steps lawyers should take to guard against disclosures, including:

- 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.

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' 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.

New York State Bar Association

Committee on Professional Ethics

Opinion 782 – 12/8/04

Topic: E-mailing documents that may contain hidden data reflecting client confidences and secrets.

Digest: Lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in “metadata” in documents they transmit electronically to opposing counsel or other third parties.

Code: DR 1-102(A)(5), 4-101(B), (C), (D); EC 4-5.

QUESTION

DR 4-101(B) states that a lawyer shall not “knowingly” reveal a confidence or secret of a client. Does a lawyer who transmits documents that contain “metadata” reflecting client confidences or secrets violate DR 4-101(B)?

OPINION

Word-processing software commonly used by lawyers, such as Microsoft Word and Corel WordPerfect, include features that permit recipients of documents transmitted by e-mail to view “metadata,” which may be loosely defined as data hidden in documents that is generated during the course of creating and editing such documents. It may include fragments of data from files that were previously deleted, overwritten or worked on simultaneously.¹ Metadata may reveal the persons who worked on a document, the name of the organization in which it was created or worked on, information concerning prior versions of the document, recent revisions of the document, and comments inserted in the document in the drafting or editing process. The hidden text may reflect editorial comments, strategy considerations, legal issues raised by the client or the lawyer, legal advice provided by the lawyer, and other

¹ David Hricik and Robert R. Jueneman, “The Transmission and Receipt of Invisible Confidential Information,” 15 The Professional Lawyer No. 1, p. 18 (Spring 2004); Mark Ward, “The hidden dangers of documents,” BBC News World Edition, August 18, 2003, at <http://news.bbc.co.uk/2/hi/technology/3154479.stm>; “Barry MacDonnell’s Toolbox for WordPerfect for Windows – Macros, Tips, and Templates,” February 5, 2004, at <http://home.earthlink.net/~wptoolbox?Tips/UndoRedo.html>.

information.² Not all of this information is a confidence or secret, but it may, in many circumstances, reveal information that is either privileged or the disclosure of which would be detrimental or embarrassing to the client. See DR 4-101. For example, a lawyer may transmit a document by e-mail to someone other than the client without realizing that the recipient is able to view prior edits and comments to the document that would be protected as privileged attorney-client communications. Or, more dramatically, a prosecutor using a cooperation agreement signed by one confidential witness may use the agreement as a template in drafting the agreement for another confidential witness. The second document's metadata could contain the name of the original cooperating witness, and if e-mailed, could expose that witness to extreme risks.

The Lawyer's Code of Professional Responsibility (the "Code") prohibits lawyers from "knowingly" revealing a client confidence or secret, DR 4-101(B)(1), except when permitted under one of five exceptions enumerated in DR 4-101(C). DR 4-101(D) states that a lawyer "shall exercise reasonable care to prevent his or her employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client." See *also* EC 4-5 ("Care should be exercised by a lawyer to prevent the disclosure of the confidences and secrets of one client to another"). Similarly, a lawyer who uses technology to communicate with clients must use reasonable care with respect to such communication, and therefore must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances. See N.Y. State 709 (1998) ("an attorney must use reasonable care to protect confidences and secrets"); N.Y. City 94-11 (lawyer must take reasonable steps to secure client confidences or secrets).

When a lawyer sends a document by e-mail, as with any other type of communication, a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information. What constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a "template" used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document. Reasonable care may, in some

² "How To: Minimize Metadata in Microsoft Word 2002 Documents," at <http://support.microsoft.com/?kbid=237361>; "How To: Minimize Metadata in Microsoft Word 2000 Documents," at <http://support.microsoft.com/?kbid=237361>. Most Word document files contain a revision log listing the last 10 edits of a document, and identifying the names of the people who worked on the document and the names of the files in which the data was saved. Richard M. Smith, "Microsoft Word bytes Tony Blair in the butt," June 30, 2003, at <http://www.computerbytesman.com/privacy/blair.htm> (describing how the British government was embarrassed in February 2003 when 10 Downing Street published a dossier on Iraq's security and intelligence organizations and posted it as a Microsoft Word document on their Web site, which through its metadata revealed the identities of the four civil servants who worked on the document as well as various other documents that contained the same information). Similarly, WordPerfect documents may contain information text that had been cut, copied or deleted, as well as the drafter's username, the drafter's initials, the company or organization name, the name of the computer, embedded objects, comments, and other file properties and summary information. "Barry MacDonnell's Toolbox for WordPerfect for Windows – Macros, Tips, and Templates," February 5, 2004, at <http://home.earthlink.net/~wptoolbox?Tips/UndoRedo.html>.

circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission. See N.Y. State 709 (1998).³

Lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets. In N.Y. State 749, we concluded that the use of computer technology to access client confidences and secrets revealed in metadata constitutes “an impermissible intrusion on the attorney-client relationship in violation of the Code.” N.Y. State 749 (2003). See *also* N.Y. State 700 (1997) (improper for a lawyer to exploit an unauthorized communication of confidential information because doing so would constitute conduct “involving dishonesty, fraud, deceit or misrepresentation” and “prejudicial to the administration of justice” in violation of DR 1-102(A)(4) and DR 1-102(A)(5), respectively).⁴

CONCLUSION

Lawyers have a duty under DR 4-101 to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets.

(1-04)

³ Some commentators have suggested that a lawyer has an affirmative duty to remove metadata whenever documents are exchanged with opposing counsel or disclosed to the public. See, e.g., David Hricik & Robert R. Jueneman, *The Transmission and Receipt of Invisible Confidential Information*, 15 *The Professional Lawyer* no. 1, p. 18 (Spring 2004) (“To comply with their duty of confidentiality, lawyers should take steps to remove metadata from documents exchanged with opposing counsel or disclosed to the public”). While exercising reasonable care under DR 4-101 may, in certain circumstances, require the lawyer to remove metadata (for example, where the lawyer knows that the metadata reflects client confidences and secrets, or that the document is being sent to an aggressive and technologically savvy adversary), in general the level of care required varies with the particular circumstances of the transmission.

⁴ Unlike lawyers, non-lawyer recipients of documents containing hidden text have no obligation imposed by the Code to avoid uncovering and exploiting information contained in an e-mailed document's metadata.

New York State Bar Association

Committee on Professional Ethics

Opinion 749 – 12/14/01

Topic: Use of computer software to surreptitiously examine and trace e-mail and other electronic documents

Digest: Lawyers may not ethically use available technology to surreptitiously examine and trace e-mail and other electronic documents.

Code: DR 1-102(A)(4), DR 1-102(A)(5), DR 4-101, DR 7-102(A)(8), Canon 4, Canon 7, EC 4-1

BACKGROUND

Modern computer technology enables sophisticated users who receive documents by electronic transmission to “get behind” what is visible on the computer screen and determine, among other things, revisions made at various stages, and sometimes even the authors of the revisions. Use of this technology would enable a lawyer who receives e-mail and electronic documents from counsel for an opposing party to obtain various kinds of information that the sender has not intentionally made available to the lawyer. For example, a lawyer who has received the final draft of a contract from counsel for a party with whom the lawyer is negotiating would be able to see prior drafts of the contract and, perhaps, learn the identity of those who made the revisions, without the knowledge or consent of the sending lawyer. How to effectively “block” recipients from access to deletions and prior versions of the “visible” document appears to be unclear and a matter of debate among sophisticated computer users. See, e.g., M. David Stone, “Deleting Your Deletions,” P.C. Magazine November 20, 2000.

It is also possible for an e-mail sender to determine the subsequent route of the e-mail, including comments on the e-mail written by its ultimate recipients. Through use of this application a lawyer can place a “bug” in e-mail he or she sends to opposing counsel and learn the identity of those with whom the first recipient shares the message and comments that these persons may make about it. Even if a user can avoid applications that make it possible to place a bug in the user’s e-mail, the recipient’s forwarded messages can still be traced if the user forwards the message to someone who has not

taken these measures. Accordingly, it is virtually impossible to render one's e-mail system "bug-proof". See www.privacyfoundation.org/privacywatch, "E-Mail Wiretapping", posted February 5, 2001.

QUESTION

May a lawyer ethically may use available technology to surreptitiously examine and trace e-mail and other electronic documents in the manner described?

OPINION

This new technology permits a user to access confidential communications relating to another lawyer's representation of a client, including "confidences" and "secrets" within the scope of DR 4-101 of the Lawyer's Code of Professional Responsibility ("Code")¹ For this reason, we conclude that the use of computer technology in the manner described above constitutes an impermissible intrusion on the attorney-client relationship in violation of the Code. The protection of the confidences and secrets of a client are among the most significant obligations imposed on a lawyer. As explained in EC 4-1:

Both the fiduciary relationship existing between lawyer and client and the proper function of the legal system require the preservation by the lawyer of confidences and secrets of one who has employed or sought to employ the lawyer. A client must feel free to discuss anything with his or her lawyer and a lawyer must be equally free to obtain information beyond that volunteered by the client. . . . The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of a client not only facilitates the full development of facts essential to proper representation of the client but also encourages non-lawyers to seek early legal assistance.

Although the precise question presented in this inquiry has not previously been answered by this Committee or, to our knowledge, by other ethics authorities, we believe the circumstances described are substantively analogous to less technologically sophisticated means of invading the attorney-client relationship that we and other authorities have addressed and rejected as inconsistent with the ethical norms of the profession. For example, the strong public policy in favor of protecting attorney-client confidentiality is expressed in the prohibition against lawyers (1) soliciting the disclosure of unauthorized communications, *see, e.g., Dubois v. Gradco Sys., Inc.*, 136 F.R.D. 341, 347 (D. Conn. 1991) (Cabranes, J.) (Although former employees of adverse corporate party are not within reach of the no-contact rule "it goes without saying that plaintiff's counsel must take care not to seek to induce or listen to disclosures by the former employees of any

¹ The Code defines "confidence" as "information protected by the attorney-client privilege under applicable law"; the term "secret" includes all "other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." DR 4-101(A).

privileged attorney-client communications to which the employee was privy”); *see also* ABA Formal Op. 91-359; (2) exploiting the willingness of others to undermine the confidentiality principle, *see* N.Y. State 700 (1997); ABA Formal Op. 94-382; and (3) making use of inadvertent disclosures of confidential communications, *see* ABA Formal Op. 92-368.

The Code prohibits a lawyer from engaging in conduct “involving dishonesty, fraud, deceit or misrepresentation,” DR 1-102(A)(4) and “conduct that is prejudicial to the administration of justice.” DR 1-102(A)(5). We believe that in light of the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship, use of technology to surreptitiously obtain information that may be protected by the attorney-client privilege, the work product doctrine or that may otherwise constitute a “secret” of another lawyer’s client would violate the letter and spirit of these Disciplinary Rules. *Accord MMR/Wallace Power & Indus. Inc. v. Thames Assocs.*, 764 F. Supp. 712, 718-19 (D. Conn. 1991) (spirit if not the letter of ethical rules precludes an attorney from acquiring, inadvertently or otherwise, confidential information about his adversary’s litigation strategy); *In re Wisehart*, 721 N.Y.S. 2d 356, 281 A.D. 2d 23, (1st Dep’t 2001) (respondent suspended for two years for using documents purloined by his client from opposing counsel); N.Y. City 1989-1 (client’s interception of adversary’s communications with counsel involved dishonesty and deceit; lawyer may not help client take advantage of such wrongdoing).

In the present inquiry, although counsel for the other party intends the lawyer to receive the “visible” document, absent an explicit direction to the contrary counsel plainly does not intend the lawyer to receive the “hidden” material or information about the authors of revisions to the document. To some extent, therefore, the “inadvertent” and “unauthorized” disclosure cases provide guidance in the present inquiry.

In N.Y. State 700 (1997), we concluded that a lawyer who receives an unsolicited and unauthorized communication from a former employee of an adversary’s law firm may not seek information from that person if the communication would exploit the adversary’s confidences or secrets. Despite the fact that the Code does not expressly require a lawyer to refrain from encouraging a breach of client confidentiality by opposing counsel’s staff, we determined that because use of such information would undermine confidentiality and the attorney-client relationship, it was conduct “involving dishonesty, fraud, deceit or misrepresentation,” DR 1-102(A)(4), and “conduct prejudicial to the administration of justice.” DR 1-102(A)(5).

In N.Y. State 700 we cited ABA Formal Op. 92-368 in support of our conclusion that the strong public policy in favor of confidentiality outweighed what might be seen as the competing principles of zealous representation (Canon 7) and encouraging more careful conduct. ABA 92-368 concluded that a lawyer who receives confidential materials under circumstances where it is clear that they were not intended for the receiving lawyer (a) should not examine the materials once the inadvertence is discovered, (b) should notify the sending lawyer of their receipt, and (c) should abide by the sending lawyer’s instructions as to their disposition.

The circumstances of the present inquiry present an even more compelling case against surreptitious acquisition and use of confidential or privileged information than that presented by the “inadvertent” or “unauthorized” disclosure decisions. First, to the extent that the other lawyer has “disclosed”, it is an unknowing and unwilling, rather than inadvertent or careless, disclosure. In the “inadvertent” and “unauthorized” disclosure decisions, the public policy interest in encouraging more careful conduct had to be balanced against the public policy in favor of confidentiality. No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets.

Nor need we balance the protection of confidentiality against the principles of zealous representation expressed in Canon 7. Our Code carefully circumscribes factual and legal representations a lawyer can make, people a lawyer may contact, and actions a lawyer can take on behalf of a client. Prohibiting the intentional use of computer technology to surreptitiously obtain privileged or otherwise confidential information is entirely consistent with these ethical restraints on uncontrolled advocacy.

Although our jurisdiction does not extend to questions of law, we note that the misuse of some aspects of this technology, particularly the use of e-mail “bugs,” may violate federal or state law prohibiting unauthorized interception of e-mail content. See, e.g., The Electronic Communications Privacy Act, 18 U.S.C. §§2510 *et. seq.* In that event, such conduct would, of course, be unethical *per se*. DR 7-102(A)(8) (“In the representation of a client, a lawyer shall not . . . [k]nowingly engage in other illegal conduct or conduct contrary to a Disciplinary Rule”).

Finally, the inquiry that has prompted this opinion underscores the need for all lawyers to exercise care in using Internet based e-mail. Accordingly, we reiterate the admonition we offered in N.Y. State 709 (1998) that “lawyers must always act reasonably in choosing e-mail for confidential communications, as with any other means of communication.”²

CONCLUSION

A lawyer may not make use of computer software applications to surreptitiously “get behind” visible documents or to trace e-mail.

(25-01)

² As noted in N.Y. State 709 (1998), “in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely within the lawyer’s control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail.”

March 29, 2022

by Arctic Wolf (<https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/>)

The Top 11 Legal Industry Cyber Attacks

11. Campbell Conroy & O’Neil P.C.

The law firm Campbell Conroy & O’Neil P.C. was subject to a data breach on February 27, 2021. The firm became aware of unusual activity, then conducted an investigation and discovered it had unwittingly been a ransomware victim.

The ransomware attack prevented Campbell Conroy & O’Neil P.C. from accessing critical files in its system. Although the full extent and impact of the attack have not yet been determined, Campbell Conroy & O’Neil P.C. speculates that the attacker had access to clients’ names, Social Security numbers, driver’s license numbers, dates of birth, and other key identifying facts.

Cyber attack type: Ransomware

Location: Boston, Massachusetts

Cost: Unknown

People and companies affected: Unknown

In response to the breach, Campbell Conroy & O’Neil P.C. contacted third-party forensic investigators to determine what information may have been compromised. Furthermore, the law firm alerted the FBI and offered its clients 24 months of

complimentary access to services such as credit monitoring, fraud consultation, and more.

10. Grubman Shire Meiselas & Sacks

In May 2020, Grubman Shire Meiselas & Sacks, which offers legal services to the entertainment and media industries, acknowledged having experienced a ransomware attack. To exert pressure, the hackers leaked information involving Lady Gaga, who is a client of the law firm. They also threatened to release information involving other celebrities.

The attackers asked for a ransom payment of \$42 million to prevent the release of the documents to the public. The perpetrators originally asked for \$21 million, then doubled their payment demand.

According to news outlets, the criminals behind the attack reported having received \$365,000 from the firm. They threatened to release additional data, much of which involves celebrities, if they didn't receive payment in full.

Cyber attack type: Ransomware

Location: Undisclosed

Cost: To be determined

People affected: To be determined

As part of its response, the firm disclosed that it has hired “the world’s experts who specialize in this area, and [is] working around the clock to address these matters.”

Previously, Travelex, a British company that provides foreign exchange services, paid the same criminal gang a \$2.3-million ransom to regain control of its files and network.

9. Fragomen, Del Rey, Bernsen & Loewy

Fragomen, Del Rey, Bernsen & Loewy confirmed it was the victim of a data breach on September 24, 2020. The law firm was heavily involved with Google, and the data breach involved personal information for both current and former Google employees.

An unauthorized third party was able to access at least one file that contained personal information on several Google employees, such as driver's license numbers and other personally identifiable information. This placed certain Google employees at risk for identity theft or other forms of fraud.

Cyber attack type: Unknown, possibly phishing scam

Location: New York

Cost: Unknown

People and companies affected: Unknown

Fragomen, Del Rey, Bernsen & Loewy filed a notice with the FBI and, even today, are still unsure how many Google employees are or were affected. The state attorney general was notified, and Google has updated its security policies for Form I-9s for employees.

Lawyer making notes inside of a book. Legal cyber attacks continue to rise at an alarming rate.

8. Oleras

In 2016, a cybercriminal using the alias Oleras allegedly targeted 50 law firms to steal confidential information to facilitate insider trading. The hacker attempted to hire accomplices via the criminal underground to help breach the law firms' defenses and then use keywords to search for pending deals

To entice others to join, Oleras advertised a plan that detailed the names, email addresses, and social media accounts of the law firm employees to be targeted.

One of the phishing emails associated with the scheme appeared to originate from a business journal asking to run a profile of the recipient about their work in mergers and acquisitions.

Cyber attack type: Phishing

Location: United States

Cost: Undisclosed

Once made aware of the threat, the FBI initiated an investigation and issued an industry alert. To date, none of the law firms targeted by Oleras have disclosed a breach in their firm's defenses.

7. Jenner & Block and Proskauer Rose

Jenner & Block admitted that in response to a request that appeared legitimate, the firm had "mistakenly transmitted" employee W-2 forms to "an unauthorized recipient" in 2017. The phishing scheme resulted in the inadvertent sharing of personal information of 859 individuals, including their Social Security numbers and salaries.

Proskauer Rose experienced a similar attack, involving what appeared to be a routine request from a senior executive within the firm. In this case, the firm lost control of more than 1,500 W-2s.

Cyber attack type: Phishing

Location: New York

Cost: Undisclosed

People affected: 2,359

Jenner & Block reported the breach to the relevant authorities. It provided two years of access to Experian's ProtectMyID Elite 3B product to employees whose information was released. It also established a hotline for former and current employees and held townhall meetings with employees to discuss the breach.

Proskauer Rose also notified authorities of the disclosure of its employees' personal information. The firm provided two years of identity recovery services for all employees, regardless of their involvement in the breach.

6. GozNym Malware

In 2016, two undisclosed law firms experienced attacks involving malware known as GozNym, which criminals used to covertly steal banking login and password information.

To trick law firm personnel into providing their banking credentials, the criminals sent a phishing email that directed the recipient to web pages designed to look like their bank's website. The scheme used keystroke logging, which recorded the keys entered when victims visited the fake bank site. It then sent that information surreptitiously to the cybercriminals.

The attack targeted bank accounts at Bank of America and Brookline Bank. Once the criminals gained access to the law firm's bank accounts, they transferred funds to other U.S. and foreign bank accounts they controlled. One law firm experienced a loss of more than \$76,000, while the other firm lost \$41,000.

Cyber attack type: Phishing and malware

Location: Washington D.C. and Wellesley, Massachusetts

Cost: \$117,000

According to the indictment, GozNym infected thousands of devices, with the potential to cause more than \$100 million in losses.

Legal books on a shelf. Law firm cyber attacks continue to rise.

5. Moses Afonso Ryan Ltd.

The law firm Moses Afonso Ryan Ltd. had its critical files locked down for three months due to a ransomware attack in 2016. Specifically, the firm's billing system and documents were frozen, so they could not be paid by clients and key financial information could not be accessed.

After the system was disabled, the law firm was forced to negotiate a ransom, which was paid in Bitcoin. In total, nearly \$700,000 was lost in client billings, as well as the undisclosed ransom cost.

Cyber attack type: Ransomware

Location: Providence, Rhode Island

Cost: At least \$700,000

People and companies affected: Unknown

Moses Afonso Ryan Ltd. was first required to pay Bitcoin up front to the hackers, then negotiate additional Bitcoin releases later. This unfortunate predicament left the firm floundering and its employees unproductive for several months.

4. Cravath Swaine & Moore and Weil Gotshal & Manges

To engage in insider trading and gather confidential information regarding pending mergers and acquisitions, three Chinese nationals targeted the law firms of Cravath Swaine & Moore and Weil Gotshal & Manges.

According to the U.S. government, Iat Hong, Bo Zheng, and Chin Hung earned over \$4 million in profits while trading on information they stole from the law firms. To gather such information, the perpetrators used their unauthorized access to read emails belonging to partners at both firms about pending transactions involving public companies.

The indictment notes the defendants targeted five additional law firms, launching at least 100,000 attacks on those firms.

Cyber attack type: Malware and other undisclosed methods

Location: New York

Cost: Undisclosed

Illegal trading profits: \$4+ million

For trading on insider information, the U.S. Securities and Exchange Commission fined the perpetrators \$8.8 million.

3. DLA Piper

In June 2017, DLA Piper suffered a ransomware attack that first struck its Ukrainian offices during an upgrade of its payroll software. The attack involved malware known as NotPetya. The firm cited its “flat network structure” as a reason the infection spread so quickly.

As a result of the attack, DLA Piper employees around the world could not use the firm’s telephones or email system, and some struggled to access certain documents. However, the firm states that it did not lose any data and its backups remained intact.

Cyber attack type: Ransomware

Location: Ukraine, then global

Cost: Millions of dollars

In response to the attack, the firm’s IT department worked 15,000 hours of paid overtime. Given the depth and severity of the attack, the firm had to wipe and rebuild its Windows environment.

2. Appleby

In 2016, Appleby, an offshore law firm located in Bermuda, experienced a cyber attack. News of the attack surfaced in 2017, when the hack attracted interest from the ICIJ.

Known as **the Paradise Papers**, the law firm's breached records included 13.4 million files. According to The Guardian, a total of 96 media companies and 381 journalists reviewed the documents.

The same journalists from Süddeutsche Zeitung who received the Panama Papers also obtained the documents in the Paradise Papers. Appleby denied the involvement of an insider, instead claiming that hackers had taken the documents.

Cyber attack type: Hack or insider attack

Location: Bermuda

Cost: Undisclosed

People and companies affected: 120,000+

In response to the breach, Appleby engaged in legal action against The Guardian and the BBC, seeking compensation for the disclosure of its legal documents. It subsequently settled the dispute by entering into a confidential agreement with both media companies.

The ICIJ reports that the Paradise Papers resulted in the recovery of unpaid taxes and assessment of penalties. The ICIJ also reports an increased awareness of the need for vigilance and more robust security to prevent future breaches.

1. Mossack Fonseca

In April 2016, journalists from German newspaper Süddeutsche Zeitung, Bastian Obermayer and Frederik Obermaier, received approximately 11.5 million documents belonging to the Panamanian law firm Mossack Fonseca.

The journalists subsequently contacted the International Consortium of Investigative Journalists (ICIJ). The ICIJ put together a team of 107 media organizations located in 76 countries to review the documents, later known as **the Panama Papers**. Among other forms of questionable activity, the documents detailed the widespread use of shell companies and complex transactions as means of committing tax fraud.

While some claim that the 11.5 million records that ended up in the hands of the world press came from a leak from an anonymous insider, Mossack Fonseca claims that the firm experienced a hack.

Cyber attack type: Hack or insider attack

Location: Panama City, Panama

Cost: The firm closed its doors in March 2018

People affected: 300,000+

In the aftermath of the Panama Papers, several individuals mentioned in the documents resigned, including Iceland's then prime minister, Sigmundur David Gunnlaugsson. Governments around the world used the documents to recover more than \$1.2 billion. As a direct result of the adverse publicity associated with the Panama Papers, Mossack Fonseca closed its doors in March 2018.

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 23-011

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

Heidell, Pittoni, Murphy & Bach LLP,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (the “OAG”) commenced an investigation pursuant to Executive Law § 63(12) and General Business Law (“GBL”) §§ 899-aa and 899-bb as well as the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (“HIPAA”) into a data security incident at Heidell, Pittoni, Murphy & Bach LLP (“HPMB” or “Respondent”) (together with the OAG, the “Parties”). This Assurance of Discontinuance (“Assurance”) contains the findings of the OAG’s investigation and the relief agreed to by the OAG and HPMB.

FINDINGS OF OAG

1. Respondent, HPMB, is a law firm based in New York, NY, that, among other things, represents hospitals and hospital networks in litigation. In connection with its role in representing hospitals and hospital networks in litigation, HPMB receives and maintains electronic protected health information (“ePHI”) and other private information related to its clients’ patients. As a result, HPMB was, at all relevant times, classified as a “Business Associate” under HIPAA and related regulations. *See* 45 C.F.R. §§ 160.103.

The 2021 Data Breach

2. On or about November 22, 2021, an attacker exploited vulnerabilities in HPMB's Hybrid Exchange Management Server to gain access to HPMB's systems. The vulnerabilities the attacker exploited had been identified by Microsoft several months earlier—in April and May 2021—and Microsoft had released patches for the software vulnerabilities around the same time. HPMB did not timely apply the patch for these vulnerabilities, rendering the server vulnerable to the attack.

3. On or around December 25, 2021, the attacker deployed the Lockbit ransomware variant on HPMB's systems using PSEXec. HPMB personnel were alerted to this intrusion on December 25, when HPMB received an internal alert relating to syncing errors. HPMB subsequently identified encryption on its network consistent with a ransomware attack.

4. In response to the attack, HPMB disconnected its servers from the internet and hired a forensic cybersecurity firm to conduct a forensic investigation. The forensic firm engaged in discussions with the attackers, who provided the forensic firm a list of tens of thousands of files the attackers claimed to have exfiltrated from HPMB's systems. This list included legal pleadings, patient lists, and medical records that HPMB had in its possession in connection with litigation matters. The forensic firm identified evidence that the listed files had been staged and exfiltrated from HPMB's systems.

5. HPMB subsequently paid \$100,000 in ransom in exchange for the return and promised deletion of the exfiltrated data but was not provided evidence the data was deleted.

6. With the aid of a contractor, HPMB engaged in an analysis of the files exfiltrated from its systems. As a result of this analysis, HPMB determined that the ePHI and/or private information—including names, dates of birth, social security numbers, and/or health data—of

114,979 individuals, including 61,438 New York residents, had likely been exposed as a result of the attack. Of this number, 846 New Yorkers had their social security numbers exposed, 23 New Yorkers had their driver's license numbers exposed, 13 New Yorkers had their other identification card details exposed, and 25 New Yorkers had their biometric data exposed.

7. On May 16, 2022, after HPMB's data-mining vendor had concluded its analysis of the exfiltrated files, Respondent began notifying affected individuals whose ePHI and private information had been exposed during the attack.

8. As a HIPAA Business Associate, HPMB must comply with the federal standards that govern the privacy and security of ePHI, as defined in 45 C.F.R. § 160.103—specifically, the HIPAA Privacy Rule and HIPAA Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E.

9. In the course of its investigation of the 2021 Data Breach, the OAG determined that HPMB failed to comply with many of the standards and procedural specifications required by HIPAA's Privacy Rule and Security Rule including, *inter alia*, the following:

- a. HPMB failed to ensure the confidentiality and integrity of all ePHI it creates, receives, maintains, or transmits, *see* 45 C.F.R. § 164.306(a)(1);
- b. HPMB failed to protect against reasonably anticipated threats or hazards to the security or integrity of such information, *see* 45 C.F.R. § 164.306(a)(2);
- c. HPMB failed to review and modify its data protection practices as needed to ensure reasonable and appropriate protection of ePHI, *see* 45 C.F.R. § 164.306(e);
- d. HPMB failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI

- it holds, *see* 45 C.F.R. § 164.308(a)(1)(ii)(A);
- e. HPMB failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a), *see* 45 C.F.R. § 164.308(a)(1)(ii)(B);
 - f. HPMB failed to implement procedures to regularly review records of information system activity, *see* 45 C.F.R. § 164.308(a)(1)(ii)(D);
 - g. HPMB failed to implement procedures sufficient to guard against, detect, and report malicious software, *see* 45 C.F.R. § 164.308(a)(5)(ii)(B);
 - h. HPMB failed to implement procedures sufficient for periodic testing and revision of contingency plans, *see* 45 C.F.R. § 164.308(a)(7)(ii)(D);
 - i. HPMB failed to perform a periodic technical and nontechnical evaluation, based upon the standards implemented under the Security Rule and in response to environmental or operational changes affecting the security of ePHI, that established the extent to which its security policies and procedures meet the requirements of 45 C.F.R. Part 164, Subpart C, *see* 45 C.F.R. § 164.308(a)(8);
 - j. HPMB failed to sufficiently implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4), *see* 45 C.F.R. § 164.312(a)(1);
 - k. HPMB failed to implement a sufficient mechanism to encrypt and decrypt ePHI, *see* 45 C.F.R. § 164.312(a)(2)(iv);
 - l. HPMB failed to implement a centralized logging system that would allow it to record and examine activity in information systems that contain ePHI, *see* 45

C.F.R. § 164.312(b);

- m. HPMB failed to implement a system to identify whether PHI has been altered or destroyed in an unauthorized manner, *see* 45 C.F.R. § 164.312(c)(2);
- n. HPMB failed to implement procedures sufficient to verify that a person or entity seeking access to ePHI is the one claimed, *see* 45 C.F.R. § 164.312(d);
- o. HPMB failed to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of 45 C.F.R. Part 164, Subpart C, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv), *see* 45 C.F.R. § 164.316(a);
- p. HPMB failed to prevent unauthorized access to the ePHI of individuals whose information was maintained on the HPMB Network, *see* 45 C.F.R. § 164.502(a); and,
- q. HPMB failed to implement reasonable and appropriate policies and procedures to comply with the “minimum necessary” requirements for ePHI requests, use, and disclosure, *see* 45 C.F.R. § 164.502(b).

10. The OAG further finds that HPMB violated GBL § 899-aa by failing to provide affected New Yorkers with timely notice of the 2021 Data Breach and GBL § 899-bb(2) by failing to adopt reasonable data security practices to protect private information.

11. Respondent neither admits nor denies OAG’s Findings, paragraphs 1-10 above.

12. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of HIPAA, *see* 42 U.S.C. § 1320d-5(d), or Executive Law § 63(12) and GBL §§ 899-aa & 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

RELIEF

13. For the purposes of this Assurance, the following definitions shall apply:
- a. “Affected Consumer” means any person who resided in New York at the time of the Security Event and whose Private Information or ePHI was potentially subject to the Security Event.
 - b. “Effective Date” shall be the date of the last signature to this agreement.
 - c. “ePHI” or “Electronic Protected Health Information” has the same meaning as the same term in 45 C.F.R. § 160.103.
 - d. “Private Information” shall have the same meaning as the same term in New York General Business Law § 899-aa.
 - e. “Security Event” means the ransomware attack that occurred in December 2021 and resulted in unauthorized access to and acquisition of Private Information and ePHI maintained by HPMB.

GENERAL COMPLIANCE

14. Respondent shall comply with Executive Law § 63(12) and GBL §§ 899-aa & 899-bb as well as HIPAA’s Privacy Rule and Security Rule, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A, C, and E, in connection with its collection, use, and maintenance of ePHI and Private Information.

INFORMATION SECURITY PROGRAM

15. Respondent shall maintain a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of the ePHI and Private Information that Respondent collects, stores, transmits,

and/or maintains. Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

- a. Assess and document, not less than annually, internal and external risks to the security, integrity and confidentiality of ePHI and Private Information;
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the ePHI and Private Information that Respondent collects, stores, transmits, and/or maintains;
- c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;
- d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;
- e. Select service providers capable of appropriately safeguarding ePHI and Private Information, contractually require service providers to implement and maintain appropriate safeguards to protect ePHI and Private Information, and take appropriate steps to verify service providers are complying with the contractual requirements;

- f. Evaluate the Information Security Program not less than annually and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

16. Respondent shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program (the "Chief Information Security Officer"). The Chief Information Security Officer shall report at a minimum quarterly to the Chief Executive Officer (or the equivalent thereof) and senior management concerning Respondent's security posture, the security risks faced by Respondent, and the Information Security Program. The Chief Information Security Officer shall report at a minimum semi-annually to the Board of Directors (or the equivalent thereof) regarding the same.

17. Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the Effective Date of this Assurance, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security Program.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

18. Encryption: Respondent shall encrypt ePHI and Private Information that it collects, uses, stores, transmits and/or maintains, whether stored within Respondent's network, or

transmitted electronically within or outside the Respondent's network, using a reasonable encryption algorithm where technically feasible.

19. Logging & Monitoring: Respondent shall, to the extent it has not already done so, establish, and, thereafter, maintain a system designed to programmatically collect and monitor network activity, such as through the use of security and event management tools, as well as policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (1) provide for centralized logging and monitoring that includes collection and aggregation of logging for Respondent's network, and (2) monitor for and alert security personnel to suspicious activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

20. Patch Management: Respondent shall implement and maintain a reasonable policy to update and patch software on its computer network including the following:

- a. Monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from software manufacturers and ensuring the appropriate and timely application of all security updates and/or security patches;
- b. Supervising, evaluating, and coordinating any system patch management tool(s); and,
- c. Training requirements for individuals responsible for implementing and maintaining Respondent's patch management policies.

21. Penetration Testing: Respondent shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within Respondent's computer network. This program shall include regular penetration testing,

risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

22. Data Collection: Respondent shall request, collect, use, or store ePHI and/or Private Information only to the minimum extent necessary to accomplish the intended legitimate business purpose for collection.

23. Data Deletion: Respondent shall permanently and securely delete or otherwise dispose of ePHI and/or Private Information when there is no reasonable business or legal purpose to retain it.

INFORMATION SECURITY PROGRAM ASSESSMENTS

24. Within one (1) year of the effective date, Respondent shall obtain a comprehensive assessment of the information security of the HPMB Network conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession (the “Third-Party Assessment”) which shall be documented (“Third-Party Assessment Report”) and provided to the OAG within two weeks of completion. Annually for five (5) years thereafter, Respondent shall obtain Third-Party Assessment Reports which shall be provided to the OAG upon request. The Third-Party Assessment Reports shall:

- a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent’s Information Security Program;
- b. Document the extent to which the identified administrative, technical and physical safeguards are appropriate based on the volume and sensitivity of the ePHI and Private Information that is at risk and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to ePHI or Private Information, or the (2)

misuse, loss, theft, alteration, destruction, or other compromise of such information; and,

- c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the Information Security Program.

CREDIT MONITORING

25. Respondent shall offer two (2) years of credit monitoring and identify theft protection services to all Affected Consumers who were impacted by the 2021 Data Breach and were not previously offered identify theft protection services.

MONETARY RELIEF

26. Respondent shall pay to the State of New York two hundred thousand dollars (\$200,000) in penalties (the “Monetary Relief Amount”). Payment of the Monetary Relief Amount shall be made in full within forty-five (45) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 23-011.

MISCELLANEOUS

27. Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 34, and agrees and acknowledges that in such event:

- a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;
- b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the effective date of this Assurance;

- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue.
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

28. If a court of competent jurisdiction determines that the Respondent has violated the Assurance, the Respondent shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

29. This Assurance is not intended for use by any third party in any other proceeding.

30. Acceptance of this Assurance by the OAG is not an approval or endorsement by the OAG of any of Respondent's policies, practices, or procedures, and the Respondent shall make no representation to the contrary.

31. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. Respondent shall include any such successor, assignment, or transfer agreement a provision that binds the successor, assignee, or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

32. Any failure by the OAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

33. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 23-011, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to the Respondent, to:

Adam M. Dlugacz, or in his absence, to the person holding the title of
Managing Partner
Heidell, Pittoni, Murphy & Bach, LLP
99 Park Avenue
New York, NY 10016
adlugacz@hpmb.com

If to the OAG, to:

Laura Mumm, Assistant Attorney General, or in her absence,
to the person holding the title of Bureau Chief Bureau of
Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov

34. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and its counsel and the OAG's own factual investigation as set forth in Findings, paragraphs (1)-(10) above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

35. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

36. The Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondent further represents and warrants that Heidell, Pittoni, Murphy & Bach, LLP, by Adam M. Dlugacz, as the signatory to this AOD, is a duly authorized officer and managing partner acting at the direction of the Executive Committee of Heidell, Pittoni, Murphy & Bach, LLP.

37. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondent's obligations under this Assurance are enduring. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

38. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis.

39. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondent violates the Assurance after its Effective Date.

40. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

41. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

42. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

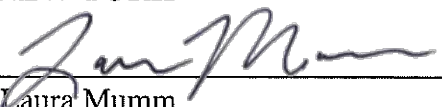
43. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

44. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

45. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

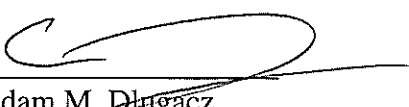
46. The Effective Date of this Assurance shall be March 10, 2023.

**LETITIA JAMES
ATTORNEY GENERAL OF THE STATE
OF NEW YORK**

By: 
Laura Mumm
Assistant Attorney General
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005
Laura.Mumm@ag.ny.gov
Phone: (212) 416-8276

Date: 3/9/2023

**HEIDELL, PITTONI, MURPHY &
BACH, LLP**

By: 
Adam M. Dlugacz
Heidell, Pittoni, Murphy & Bach, LLP
99 Park Avenue
New York, NY 10016
adlugacz@hpmb.com
Phone: (212) 286-8585

Title: Managing Partner

Date: 3/3/23

Security Incident March 2023 Update & Actions - LastPass

Karim Toubba

To Our LastPass Customers—

I want to share with you an important update about the security incident we disclosed on December 22, 2022. We have now completed an exhaustive investigation and have not seen any threat-actor activity since October 26, 2022.

During the course of our investigation, we have learned a great deal more about what happened and are sharing new findings today. Over the same period, we invested a significant amount of time and effort hardening our security while improving overall security operations. In today's update, I'll review those measures and highlight additional security steps that we are taking.

This update is structured as follows:

What happened and what actions did we take?

What data was accessed?

What actions should you take to protect yourself or your business?

What we have done to secure LastPass

What you can expect from us

We are privileged to serve millions of users and more than 100,000 businesses, and we want to ensure that all of our customers have the information they need to answer their questions. Given the volume of information we are sharing today, we have structured this update with summaries that include embedded links to provide more detailed information on each topic.

We have heard and taken seriously the feedback that we should have communicated more frequently and comprehensively throughout this process. The length of the investigation left us with difficult trade-offs to make in that regard, but we understand and regret the frustration that our initial communications caused for both the businesses and consumers who rely on our products. In sharing these additional details today, and in our approach going forward, we are determined to do right by our customers and communicate more effectively.

If you would prefer to skip ahead to review LastPass's recommended actions for protecting your account or your business, please [click here for consumers](#) or [click here for business](#) administrators.

WHAT HAPPENED AND WHAT ACTIONS DID WE TAKE?

The two incidents that we disclosed last year affected LastPass and our customers. Neither incident was caused by any LastPass product defect or unauthorized access to – or abuse of – production systems. Rather, the threat actor exploited a vulnerability in third-party software, bypassed existing controls, and eventually accessed non-production development and backup storage environments.

We have shared technical information, Indicators of Compromise (IOCs), and threat actor tactics, techniques, and procedures (TTPs) with law enforcement and our threat intelligence and forensic partners. To date, however, the identity of the threat actor and their motivation remains unknown. There has been no contact or demands made, and there has been no detected credible underground activity indicating that the threat actor is actively engaged in marketing or selling any information obtained during either incident.

Incident 1 Summary: A software engineer's corporate laptop was compromised, allowing the unauthorized threat actor to gain access to a cloud-based development environment and steal source code, technical information, and certain LastPass internal system secrets. No customer data or vault data was taken during this incident, as there is no customer or vault data in the development environment. We declared this incident closed but later learned that information stolen in the first incident was used to identify targets and initiate the second incident.

In response to the first incident, we mobilized our internal security teams, as well as resources from Mandiant. As part of the containment, eradication, and recovery process, we took the following actions:

Removed the development environment and rebuilt a new one to ensure full containment and eradication of the threat actor.

Deployed additional security technologies and controls to supplement existing controls.

Rotated all relevant cleartext secrets used by our teams and any exposed certificates.

Details of the first incident and our remediation actions can be found [here](#).

Incident 2 Summary: The threat actor targeted a senior DevOps engineer by exploiting vulnerable third-party software. The threat actor leveraged the vulnerability to deliver malware, bypass existing controls, and ultimately gain unauthorized access to cloud backups. The data accessed from those backups included system configuration data, API secrets, third-party integration secrets, and encrypted and unencrypted LastPass customer data.

In response to the second incident, we again mobilized our incident response team and Mandiant. As part of our ongoing containment, eradication, and recovery activities related to the second incident, we have taken the following actions:

Analyzed LastPass cloud-based storage resources and applied additional policies and controls.

Analyzed and changed existing privileged access controls.

Rotated relevant secrets and certificates that were accessed by the threat actor.

Additional details of the attack and our remediation actions can be found [here](#).

WHAT DATA WAS ACCESSED?

As detailed in the incident summaries, the threat actor stole both LastPass proprietary data and customer data, including the following:

Summary of data accessed in Incident 1:

On-demand, cloud-based development and source code repositories – this included 14 of 200 software repositories.

Internal scripts from the repositories – these contained LastPass secrets and certificates.

Internal documentation – technical information that described how the development environment operated.

Summary of data accessed in Incident 2:

DevOps Secrets – restricted secrets that were used to gain access to our cloud-based backup storage.

Cloud-based backup storage – contained configuration data, API secrets, third-party integration secrets, customer metadata, and backups of all customer vault data. All sensitive customer vault data, other than URLs, file paths to installed LastPass Windows or macOS software, and certain use cases involving email addresses, were encrypted using our Zero knowledge model and can only be decrypted with a unique encryption key derived from each user’s master password. As a reminder, end user master passwords are **never** known to LastPass and are not stored or maintained by LastPass – therefore, they were not included in the exfiltrated data.

Backup of LastPass MFA/Federation Database – contained copies of LastPass Authenticator seeds, telephone numbers used for the MFA backup option (if enabled), as well as a split knowledge component (the K2 “key”) used for LastPass federation (if enabled). This database was encrypted, but the separately-stored decryption key was included in the secrets stolen by the threat actor during the second incident.

Detailed information about the specific customer data impacted by these incidents can be found [here](#).

WHAT ACTIONS SHOULD YOU TAKE TO PROTECT YOURSELF OR YOUR BUSINESS?

To better assist our customers with their own incident-response efforts, we have prepared two

Security Bulletins – one for our Free, Premium, and Families consumer users, and one tailored for our Business and Teams users. Each Security Bulletin includes information designed to help our customers secure their LastPass account and respond to these security incidents in a way that we believe meets their own personal needs or their organization’s security profile and environment.

Security Bulletin: Recommended Actions for LastPass Free, Premium, and Families

This bulletin guides our Free, Premium, and Families customers through a review of important LastPass settings designed to help secure their accounts by confirming best practices are being followed.

Security Bulletin: Recommended Actions for LastPass Business This bulletin guides administrators for our Business and Teams customers through a risk assessment of LastPass account configurations and third-party integrations. It also includes information that is relevant to both non-federated and federated customers.

If you have any questions regarding the recommended actions, please contact technical support or your customer success team, both of whom are ready to help.

WHAT WE HAVE DONE TO SECURE LASTPASS

Since August, we have deployed several new security technologies across our infrastructure, data centers, and our cloud environments to further bolster our security posture. Much of this was already planned and was done in record time, as we had begun these efforts prior to the first incident.

We have also prioritized and initiated significant investments in security, privacy, and operational best practices. We have performed a comprehensive review of our security policies and incorporated changes to restrict access and privilege, where appropriate. We completed a comprehensive analysis of existing controls and configurations, and we’ve made the necessary changes to harden existing environments. We have also begun the work to expand the use of encryption within our application and backup infrastructure. Finally, we have begun to scope out longer-term architectural initiatives to help drive our platform evolution across LastPass.

You can click [here](#) to see a list of the work that has been completed and work that is currently on our security roadmap.

WHAT YOU CAN EXPECT FROM US GOING FORWARD

Since our December 22nd post, I have spoken to many of our business and consumer customers. I acknowledge our customers’ frustration with our inability to communicate more immediately, more clearly, and more comprehensively throughout this event. I accept the criticism and take full responsibility. We have learned a great deal and are committed to communicating more effectively

going forward. Today's update is a demonstration of that commitment.

Just over a year ago, GoTo and its investors announced that LastPass would become an independent company with a new leadership team. Our goal is to unlock the company's full potential and deliver on the promise of building the leading enterprise password-management platform. In late April 2022, I joined as CEO to help lead this effort.

Over the past eight months, we have hired new leaders to help drive the company's growth and execute a new strategy. Our new team includes recognized industry veterans and leaders from the security and technology industries. As part of the company's next phase of growth, we made a multi-million-dollar allocation to enhance our investment in security across people, processes, and technology. This investment drives our commitment to evolve LastPass into a leading cyber security company and ensure that we are in a position to protect ourselves and our customers against future threats.

Thank you for your understanding, guidance, and continued support.

Karim Toubba

CEO, LastPass

CYBER INSURANCE

Recovering from a cyber attack can be costly.

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider.

WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?



Make sure your policy includes coverage for:

- ☐ Data breaches (like incidents involving theft of personal information)
- ☐ Cyber attacks on your data held by vendors and other third parties
- ☐ Terrorist acts
- ☐ Cyber attacks (like breaches of your network)
- ☐ Cyber attacks that occur anywhere in the world (not only in the United States)

Also, consider whether your cyber insurance provider will:

- ☐ Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- ☐ Provide coverage in excess of any other applicable insurance you have
- ☐ Offer a breach hotline that's available every day of the year at all times

WHAT IS **FIRST-PARTY COVERAGE** AND WHAT SHOULD YOU LOOK FOR?

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business's costs related to:

- ☐ Legal counsel to determine your notification and regulatory obligations
- ☐ Customer notification and call center services
- ☐ Crisis management and public relations
- ☐ Forensic services to investigate the breach
- ☐ Recovery and replacement of lost or stolen data
- ☐ Lost income due to business interruption
- ☐ Cyber extortion and fraud
- ☐ Fees, fines, and penalties related to the cyber incident

WHAT IS **THIRD-PARTY COVERAGE** AND WHAT SHOULD YOU LOOK FOR?

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- ☐ Payments to consumers affected by the breach
- ☐ Claims and settlement expenses relating to disputes or lawsuits
- ☐ Losses related to defamation and copyright or trademark infringement
- ☐ Costs for litigation and responding to regulatory inquiries
- ☐ Other settlements, damages, and judgments
- ☐ Accounting costs

More insurance resources for small businesses available at www.insureuonline.org/smallbusiness



Cybersecurity for Small Business

PROTECT YOUR SMALL BUSINESS

CYBERSECURITY FOR

SMALL BUSINESS

Learn the basics for protecting your business from cyber attacks. The business cybersecurity resources in this section were developed in partnership with the National Institute of Standards and Technology, the U.S. Small Business Administration, and the Department of Homeland Security.



[Cybersecurity Basics](#)



[Business Email Imposters](#)



[Cyber Insurance](#)



[Email Authentication](#)



[Hiring a Web Host](#)



[Understanding the NIST Cybersecurity Framework](#)



[Phishing](#)



[Physical Security](#)



[Ransomware](#)



[Secure Remote Access](#)



[Tech Support Scams](#)



[Vendor Security](#)

Additional Resources

Check out these additional resources like downloadable guides to test your cybersecurity know-how.





[Guide for Employers](#)

[Start a Discussion](#)



[Cybersecurity Quizzes](#)

[Test Your Knowledge](#)



[Get the Materials](#)

[Download Materials](#)

[Order Free Publications](#)



[Cybersecurity Video Series](#)

[See All Topics](#)



[More FTC Small Business](#)

[Go to \[FTC.gov/SmallBusiness\]\(https://www.ftc.gov/SmallBusiness\)](#)



[Sign up to Receive the FTC Business Blog](#)

[Sign Up](#)



**FEDERAL TRADE
COMMISSION**

NIST
**National Institute of
Standards and Technology**
U.S. Department of Commerce





U.S. Small Business
Administration



Homeland
Security

J. Patrick DeLince, Esq.

J. Patrick DeLince is a private practitioner with his own law firm, *DeLince Law PLLC*. His practice concentrates on employment discrimination and business law matters. He is a graduate of St. John's University School of Law and has been practicing law in New York for more than three decades. Immediately before establishing his own practice, he managed the New York branch office of the French law firm of *Thieffry & Associates*, for which he advised American subsidiaries of French companies doing business in the United States. He has also previously worked as a Senior Staff Counsel at *Tutoki & Levy*, an *of counsel* firm to ITT Hartford.



Patrick served on the New York County Lawyers' Association's ("NYCLA") Cyberspace Law Committee as chair and on its Executive Committee, from 2000-2011, during the Internet's developmental years. At NYCLA, he also served on the Panel of Mediators and Arbitrators for Joint Committee for Fee Disputes & Conciliation (the "Panel"). The Panel's goal is to provide a private and economical means of resolving disputes between lawyers and clients. He has also had the honor of serving four times on the New York County Democratic Judicial Screening Panel.

Patrick is also a former Vice President of the Board of National Employment Lawyers Association, New York Chapter ("NELA"), and a former chair of NELA's Judiciary Committee, and its E-Discovery Committees. Currently, he serves as a board member on NELA's Shelley Leinhardt Fund.

Contact

www.linkedin.com/in/jrebholz
(LinkedIn)

Top Skills

Computer Security
Vulnerability Assessment
Information Security Management

Languages

English

Jason Rebholz

The TeachMeCyber Guy | I'll help you learn cyber security | CISO,
Adviser, Speaker, Mentor
McLean, Virginia, United States

Summary

Jason Rebholz is a cyber security leader passionate about dissecting complex problems and building programs from the ground up. His diverse experience in security start-ups contributes to his approach in leading and developing high-performing teams in fast-paced environments.

After spending a decade responding to sophisticated hacks, his professional mission evolved to solving cyber security at scale. In his current role as Chief Information Security Officer at Corvus Insurance, Jason blends his security expertise with cyber insurance to improve the security of thousands of companies.

Experience

Corvus Insurance

Chief Information Security Officer

June 2021 - Present (1 year 10 months)

As a member the Senior Leadership team, Jason splits his responsibilities between the following functions:

- Internal Security: Jason is responsible for defining and executing on a vision to secure the environment.
- Product: Jason works closely with product, data science, and engineering teams to develop and execute a vision for a risk management platform. This includes passive security scanning technology and policyholder platform.

NetDiligence®

Advisor

July 2021 - Present (1 year 9 months)

MOXFIVE

4 years 1 month

Advisor

June 2021 - Present (1 year 10 months)

McLean, Virginia, United States

Co-Founder and Chief Operating Officer

March 2019 - June 2021 (2 years 4 months)

McLean, Virginia, United States

MOXFIVE is a Technical Advisory firm that helps organizations minimize the impact of current and future security incidents through strategic security initiatives and programs and incident management services. As the co-founder and COO of MOXFIVE, Jason defined the vision and built the foundation of MOXFIVE's Incident Management and Business Resilience services that help organizations bridge the gap between IT, Security, and Business leaders to drive better outcomes before, during, and after security incidents.

Gigamon

Senior Director of Channel Services

July 2018 - March 2019 (9 months)

After Gigamon acquired ICEBRG in July 2018, Jason led company-wide initiatives to assist with the integration of the two companies. These included expanding strategic partnerships, leading the Insight Channel GTM efforts, and building services powered by Gigamon technology that were delivered through Channel partners.

ICEBRG (acquired by Gigamon)

Vice President of Strategic Partnerships

January 2018 - July 2018 (7 months)

After building incident response teams, Jason become a key member of the ICEBRG leadership team. In his role at ICEBRG, Jason led the Strategic Partnership team to build, manage, and expand key partnerships with incident response firms who leveraged ICEBRG's network detection and response technology in investigations. Through these partnerships, Jason built a reliable sales funnel that supported the growth of the company through acquisition. Having completed the critical phase of integration, Jason left to co-found MOXFIVE.

The Crypsis Group

Vice President of Professional Services

March 2016 - January 2018 (1 year 11 months)

McLean, VA

As a core member of the leadership team, Jason built the foundation of Crypsis's consulting services organization specializing in incident response. His areas of responsibility included recruiting and leading a team of 20+ consultants, driving thought leadership, and delivered cost effective incident response services for the cyber insurance industry,

Mandiant

Manager

April 2010 - March 2016 (6 years)

Washington D.C. Metro Area

Jason led incident response investigations across numerous industries including the defense industrial base, financial industry, healthcare industry, Fortune 100 companies, and law enforcement. He became an expert conducting investigations into APT threat actors, financial crime, and hackers.

In addition to his day to day activities in responding to incidents, Jason also led training sessions for audiences in law enforcement, the federal government, and corporate security groups. He also helped organizations develop and improve incident response procedures and policies to assist in the detection and remediation of security incidents.

Jason served as the regional incident response functional lead dedicated to continuous improvement of incident response processes and technologies to continue to support Mandiant's clients.

Rochester Institute of Technology

3 years 2 months

Information Security Engineer Associate

January 2009 - February 2010 (1 year 2 months)

Jason was responsible for conducting vulnerability scans of the campus network to help secure the environment.

Senior Resident Advisor

January 2007 - February 2010 (3 years 2 months)

Education

Rochester Institute of Technology

Network Security and Systems Administration · (2006 - 2010)