Hawke McKeon & Sniscak LLP
ATTORNEYS AT LAW

Thomas J. Sniscak
(717) 703-0800
tjsniscak@hmslegal.com

Kevin J. McKeon
(717) 703-0801
kjmckeon@hmslegal.com

Whitney E. Snyder
(717) 703-0807
wesnyder@hmslegal.com

100 North Tenth Street, Harrisburg, PA 17101 Phone: 717.236.1300 Fax: 717.236.4841 www.hmslegal.com

April 17, 2019

VIA ELECTRONIC FILING

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, Filing Room
Harrisburg, PA 17120

Re: Meghan Flynn, et al. v. Sunoco Pipeline L.P.; Docket Nos. C-2018-3006116 and P-2018-3006117; **SUNOCO PIPELINE L.P.'S MOTION FOR AMENDED PROTECTIVE ORDER**

Dear Secretary Chiavetta:

Enclosed for filing with the Pennsylvania Public Utility Commission is Sunoco Pipeline L.P.'s Motion for Amended Protective Order in the above-referenced proceeding.

If you have any questions regarding this filing, please contact the undersigned.

Very truly yours,

Thomas J. Sniscak

Thomas J. Sniscak
Kevin J. McKeon
Whitney E. Snyder
Counsel for Sunoco Pipeline L.P.

WES/das
Enclosure
cc: Per Certificate of Service
Honorable Elizabeth H. Barnes (ebarnes@pa.gov)
James J. Byrne, Esquire (jjbyrne@mbmlawoffice.com)
Kelly S. Sullivan, Esquire (ksullivan@mbmlawoffice.com)
Michael P. Pierce, Esquire (mppierce@pierceandhughes.com)
Joel L. Frank, Esquire (jfrank@lambmcerlane.com)

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

MEGHAN FLYNN ROSEMARY FULLER MICHAEL WALSH NANCY HARKINS GERALD MCMULLEN CAROLINE HUGHES and MELISSA HAINES	:	
Complainants,	: Docket Nos.	C-2018-3006116 P-2018-3006117
v.	:	
SUNOCO PIPELINE L.P.,	:	
Respondent.	:	

MOTION FOR AMENDED PROTECTIVE ORDER

TO THE HONORABLE ADMINISTRATIVE LAW JUDGE ELIZABETH BARNES:

Sunoco Pipeline L.P. ("SPLP") hereby requests that the Honorable Administrative Law Judge Elizabeth Barnes (the "ALJ") enter an Amended Protective Order (attached as Attachment A)[1] in these proceedings (and any proceedings consolidated with this proceeding in the future) pursuant to 52 Pa. Code §§ 5.362(a)(7) and 5.365(a). SPLP requests the Protective Order be amended to designate a third category of information that for discovery purposes will only be provided via proctored, in-person review. Under the Commission's rules of discovery, SPLP is required to serve responses (to the extent it will or will be required to respond) on all parties. Certain information Complainant's have requested in discovery is Confidential Security Information of an extremely sensitive nature. There are currently ten intervenors to this

[1] Attachment B is a redline copy of the Amended Protective Order showing the changes from the November 28, 2018 Protective Order in this case.

proceeding. Thus, SPLP would be disseminating such information to over eleven different parties, with multiple lawyers and multiple outside experts then receiving certain extremely sensitive information. For certain Confidential Security Information of an extremely sensitive nature, SPLP is not willing to disseminate this information to such a large group of people, given the potential for electronic security breaches[2], cyberattacks[3,4], and simple human error. Simply put, the sheer number of parties amplifies the risks of data breaches exposing what the Commission recognizes as highly confidential security information revolving around infrastructure security and national security. A breach of this type of information could greatly endanger the public and national security.

In support of this Motion, SPLP states as follows:

1. On November 19, 2018, Complainants filed a Formal Complaint (Docket No. C-2018-3006116) and a Petition for Interim Emergency Relief (Docket No. P-2018-3006117) with the Pennsylvania Public Utility Commission ("Commission").

2. On November 28, 2019, ALJ Barnes issued the current Protective Order in this proceeding. The Protective Order designates two categories of proprietary information, CONFIDENTIAL, and HIGHLY CONFIDENTIAL PROTECTED MATERIALS. Under the Protective Order, HIGHLY CONFIDENTIAL PROTECTED MATERIALS may only be provided

---

[2] The American Bar Association has, on many occasions, recognized the threat of electronic data breaches or cyberattacks on law firms. Most recently, by formal Opinion 483: "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." Lawyers' Obligations After An Electronic Data Breach Or Cyberattack, ABA Formal Op. 18-483 (attached as Attachment C).

[3] "The FBI has reported that law firms are often viewed as "one-stop shops" for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more)." ABA 2018 Cybersecurity techreport. David G. Ries. January 28, 2019. (attached as Attachment D).

[4] "Significantly, 23% of respondents overall reported this year that their firm had experienced a data breach at some time." *Id.*

to Reviewing Representatives (counsel and outside experts hired for purposes of this proceeding), pursuant to the terms of that order.

3. The Protective Order was entered in the context of an emergency proceeding, prior to the granting of voluminous interventions and prior to discovery. On March 1, 2019, Complainants propounded 260 interrogatories on SPLP with accompany requests for documents for 35 of those interrogatories. Those requests for production of documents include requests that implicate Confidential Security Information, some of which is extremely sensitive and if disseminated could results in providing bad actors, such as terrorists, information to harm SPLP's facilities and the public. That is not in the public interest and is contrary to the intent of state and federal law protecting such information. *E.g.*, Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6); 49 U.S.C. § 60138 (protecting certain information contained in facility response plans).

4. Under the Commission's rules of discovery, SPLP is required to serve responses (to the extent it will or will be required to respond) on all parties. There are currently ten intervenors to this proceeding. Thus, SPLP would be disseminating information to over eleven different parties, with multiple lawyers and multiple outside experts then receiving certain extremely sensitive information. For certain Confidential Security Information of an extremely sensitive nature, SPLP is not willing to disseminate this information to such a large group of people, given the potential for electronic security breaches[5], cyberattacks[6,7], and simple human error. Simply put, the shear number of parties amplifies the risks of data breaches exposing what the Commission recognizes as highly confidential security information revolving around

[5] Supra footnote 2
[6] Supra footnote 3
[7] Supra footnote 4

infrastructure security and national security. A breach of this type of information could greatly endanger the public and national security.

5. For example, in Complainant Interrogatory Set 1, No. 225, Complainant has requested SPLP to:

> Identify any estimated or calculated impact to health, safety, or the environment from potential fires or explosions due to Mariner East pipeline integrity incidents, including without limitation all calculations of the "potential impact radius" as the term is defined in Title 49 of the Code of Federal Regulations, and any measurements of the geographic area falling within the potential impact radius for each point along the pipelines.

The requested information is exactly the type of information that if disclosed to an actor with malignant intent could place SPLP's facilities and the public at risk. This request interpreted broadly would illicit information concerning the most vulnerable areas of the pipelines that could be attacked and the areas that if attacked would have the greatest impact on the public. This is information that SPLP cannot simply provide to eleven separate counsels that may then disseminate such information to a larger group.

6. Instead, in the attached Amended Protective Order, SPLP will make this type of information available to Reviewing Representatives pursuant to the terms of the Amended Protective Order at the offices of Manko, Gold, Katcher, and Fox in Bala Cynwyd, PA. After review, if a Reviewing Representative deems it necessary to have a copy of such document as part of their presentation of evidence in this proceeding, they can request a copy from counsel for Sunoco Pipeline L.P. SPLP will not be unreasonably withhold such documents subject to that Reviewing Representative confirming it understands and will abide by the terms of the Amended Protective Order concerning use of such materials.

7. Treatment of such information as set forth in the attached proposed Protective Order is justified because unrestricted disclosure of such information would not be in the public

interest. These considerations constitute cause for the restrictions specified in 52 Pa. Code § 5.365 and in Administrative Law Judge or Commission Orders granting relief pursuant to said regulation.

8. Under 52 Pa. Code §§ 5.362(a)(7) and 5.365, the Office of Administrative Law Judge or the Commission may issue a Protective Order to limit or prohibit disclosure of confidential commercial information where the potential harm to a participant would be substantial and outweighs the public's interest in having access to the confidential information. In applying this standard, relevant factors to be considered include: the extent to which disclosure would cause unfair economic or competitive damage; the extent to which the information is known by others and used in similar activities; and the worth or value of the information to the party and to the party's competitors. 52 Pa. Code § 5.365(a)(1)-(3).

9. Moreover, the Commission has an affirmative duty to protect from release Confidential Security Information, which is not subject to disclosure to third parties under the provisions and procedures specified in the 'The Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6) and the PUC's regulations implementing such Act at 52 Pa. Code §§ 102.1 – 102.4.

10. Paragraph 17 of the attached proposed Protective Order protects against overly broad designations of protected information by giving all parties the right to question or challenge the confidential or proprietary nature of the information deemed "CONFIDENTIAL," "HIGHLY CONFIDENTIAL PROTECTED MATERIAL," or "EXTREMELY SENSITIVE MATERIALS."

11. Limitation on the disclosure of information deemed "EXTREMELY SENSITIVE MATERIALS" will not prejudice the rights of the participants, nor will such limitation frustrate the prompt and fair resolution of these proceedings. The proposed Amended Protective Order balances the interests of the parties, the public, and the Commission.

12. The attached Amended Protective Order will protect Confidential Security Information and other confidential information while allowing the parties to use such information for purposes of the instant litigation. The proposed Amended Protective Order applies the least restrictive means of limitation that will provide the necessary protections from disclosure.

WHEREFORE, for all the reasons set forth above, Sunoco Pipeline L.P. respectfully requests that Your Honor issue the attached Amended Protective Order.

Respectfully submitted,

/s/Thomas J. Sniscak
Thomas J. Sniscak, Attorney I.D. # 33891
Kevin J. McKeon, Attorney I.D. # 30428
Whitney E. Snyder, Attorney I.D. # 316625
Hawke McKeon & Sniscak, LLP
100 North Tenth Street
Harrisburg, PA 17101
(717) 236-1300
tjsniscak@hmslegal.com
kjmckeon@hmslegal.com
wesnyder@hmslegal.com

/s/ Robert D. Fox
Robert D. Fox, Esq. (PA ID No. 44322)
Neil S. Witkes, Esq. (PA ID No. 37653)
Diana A. Silva, Esq. (PA ID No. 311083)
MANKO GOLD KATCHER & FOX, LLP
401 City Avenue, Suite 901
Bala Cynwyd, PA 19004
Tel: (484) 430 5700
rfox@mankogold.com
nwitkes@mankogold.com
dsilva@mankogold.com

Dated: April 17, 2019

Attorneys for Respondent Sunoco Pipeline L.P.

ATTACHMENT A

(Amended Protective Order)

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

MEGHAN FLYNN ROSEMARY FULLER MICHAEL WALSH NANCY HARKINS GERALD MCMULLEN CAROLINE HUGHES and MELISSA HAINES	Docket No.	C-2018-3006116 P-2018-3006117
Complainants,		
v.		
SUNOCO PIPELINE L.P.,		
Respondent.		

AMENDED PROTECTIVE ORDER

AND NOW, upon due consideration of the unopposed Motion for Amended Protective Order that was filed by Sunoco Pipeline L.P. on April 17, 2019;

IT IS ORDERED THAT:

1. The Motion is hereby granted with respect to all materials and information identified in Paragraphs 2 – 3 below that have been or will be filed with the Commission, produced in discovery, or otherwise presented during the above-captioned proceedings and all proceedings consolidated therewith.

2. The information subject to this Protective Order is all correspondence, documents, data, information, studies, methodologies and other materials, furnished in these proceedings, which are believed by the producing party to be of a proprietary or confidential nature and which are so designated by being marked "CONFIDENTIAL," "HIGHLY CONFIDENTIAL PROTECTED MATERIAL," or "EXTREMELY SENSITIVE MATERIALS." Such materials will be referred to below as "Proprietary Information." When a statement or exhibit is identified

for the record, the portions thereof that constitute Proprietary Information shall be designated as such for the record.

3. This Protective Order applies to the following categories of materials: (a) the parties may designate as "CONFIDENTIAL" those materials that customarily are treated by that party as sensitive or proprietary, which are not available to the public, and which, if disclosed freely, would subject that party or its clients to risk of competitive disadvantage or other business injury; (b) the parties may designate as "HIGHLY CONFIDENTIAL PROTECTED MATERIAL" those materials that are of such a commercially sensitive nature among the parties or of such a private, personal nature that the producing party is able to justify a heightened level of confidential protection with respect to those materials. Moreover, information subject to protection under the Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6) and PUC Regulations at 52 Pa. Code §§ 102.1-102.4 will also be designated as "HIGHLY CONFIDENTIAL PROTECTED MATERIAL"; (c) the parties may designate as "EXTREMELY SENSITIVE MATERIALS" those materials that are subject to protection under the Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6) and PUC Regulations at 52 Pa. Code §§ 102.1-102.4 and are of such an extremely sensitive security nature that the producing party is able to justify a heightened level of confidential protection with respect to those materials. The parties shall endeavor to limit their designation of information as HIGHLY CONFIDENTIAL PROTECTED MATERIAL and EXTREMELY SENSITIVE MATERIALS.

4. Proprietary Information shall be made available to counsel for a party, subject to the terms of this Protective Order. Such counsel shall use or disclose the Proprietary Information only for purposes of preparing or presenting evidence, cross examination, argument, or settlement in these proceedings. To the extent required for participation in these proceedings, counsel for a party may afford access to Proprietary Information subject to the conditions set forth in this Protective Order.

5. Information deemed as "CONFIDENTIAL" shall be made available to a "Reviewing Representative" who is a person that has signed a Non-Disclosure Certificate attached as Appendix A, and who is:

(i) An attorney who has entered an appearance in these proceedings for a party;

(ii) Attorneys, paralegals, and other employees associated for purposes of this case with an attorney described in Paragraph 5(i);

(iii) An expert or an employee of an expert retained by a party for the purpose of advising, preparing for or testifying in these proceedings; or

(iv) Employees or other representatives of a party appearing in these proceedings with significant responsibility for this docket.

6. Information deemed as "HIGHLY CONFIDENTIAL PROTECTED MATERIAL", may be provided to a "Reviewing Representative" who has signed a Non-Disclosure Certificate attached as Appendix A and who is:

(i) An attorney for a statutory advocate pursuant to 52 Pa. Code §1.8 or a counsel who has entered an appearance in these proceedings for a party;

(ii) An attorney, paralegal, or other employee associated for purposes of this case with an attorney described in Paragraph (i);

(iii) An outside expert or an employee of an outside expert retained by a party for the purposes of advising, preparing for or testifying in these proceedings; or

(iv) A person designated as a Reviewing Representative for purposes of HIGHLY CONFIDENTIAL PROTECTED MATERIAL, provided that a Reviewing Representative for purposes of HIGHLY CONFIDENTIAL PROTECTED MATERIAL shall not include an officer, director, stockholder, partner, or owner of any competitor of the parties, or of any shipper, customer or consignee of any affiliate of any competitor of the parties, or shipper, customer or consignee, or any employee of any such entity, if the employee's duties involve marketing or pricing responsibilities, or any responsibility for marketing or pricing with respect to the transportation or commodity sales and/or exchanges of refined petroleum products.

Provided, further, that in accordance with the provisions of Sections 5.362 and 5.365(e) of the Commission's Rules of Practice and Procedure, 52 Pa. Code §§ 5.362, 5.365(e), any party may, by subsequent objection or motion, seek further protection with respect to HIGHLY CONFIDENTIAL PROTECTED MATERIAL, including, but not limited to, total prohibition of disclosure or limitation of disclosure only to particular persons or parties.

7. Information deemed as "EXTREMELY SENSITIVE MATERIALS" may be provided to the same persons constituting Reviewing Representatives under paragraph 6 of this Order. However, such information will only be provided through in-person review at the offices of Manko, Gold, Katcher & Fox, 401 City Avenue, Suite 901, Bala Cynwyd, PA 19004, between the hours of 9AM to 5PM, Monday – Friday. Request to view such information shall be made to Diana Silva via email (dsilva@mankogold.com) at least 24-hours prior to the requested viewing session. Such review may be proctored and Reviewing Representatives are prohibited from reproducing such information in any form without the prior authorization of SPLP's counsel (including taking detailed notes or cell phone pictures). If a party determines that it is necessary to use an EXTREMELY SENSITIVE MATERIALS as part of their presentation of evidence in this proceeding, such party shall request a copy from counsel for Sunoco Pipeline L.P., which permission shall not be unreasonably withheld and subject to that party confirming it understands and will abide by the terms of this Protective Order concerning use of such materials.

8. For purposes of this Protective Order, a Reviewing Representative may not be a "Restricted Person."

(a) A "Restricted Person" shall mean: (i) an officer, director, stockholder, partner, or owner of any competitor of the parties or an employee of such an entity if the employee's duties involve marketing or pricing of the competitor's products or services; (ii) an officer, director, stockholder, partner, or owner of any affiliate of a competitor of the parties (including any association of competitors of the parties) or an employee of such an entity if the employee's duties involve marketing or pricing of the competitor's products or services; (iii) an officer, director, stockholder, owner or employee of a competitor of a customer of the parties if the Proprietary Information concerns a specific, identifiable customer of the parties; and (iv) an officer, director, stockholder, owner or employee of an affiliate of a competitor of a customer of the parties if the Proprietary Information concerns a specific, identifiable customer of the parties; provided, however, that no expert shall be disqualified on account of being a stockholder, partner, or owner unless that expert's interest in the business would provide a significant motive for violation of the limitations of permissible use of the Proprietary Information. For purposes of this Protective Order, stocks, partnership or other ownership interests valued at more than

$10,000 or constituting more than a 1% interest in a business establishes a significant motive for violation.

(b) If an expert for a party, another member of the expert's firm or the expert's firm generally also serves as an expert for, or as a consultant or advisor to, a Restricted Person, said expert must: (i) identify for the parties each Restricted Person and each expert or consultant; (ii) make reasonable attempts to segregate those personnel assisting in the expert's participation in this proceeding from those personnel working on behalf of a Restricted Person; and (iii) if segregation of such personnel is impractical the expert shall give to the producing party written assurances that the lack of segregation will in no way jeopardize the interests of the parties or their customers. The parties retain the right to challenge the adequacy of the written assurances that the parties' or their customers' interests will not be jeopardized. No other persons may have access to the Proprietary Information except as authorized by order of the Commission.

8. A qualified "Reviewing Representative" for "HIGHLY CONFIDENTIAL PROTECTED MATERIAL" may review and discuss "HIGHLY CONFIDENTIAL PROTECTED MATERIAL" with their client or with the entity with which they are employed or associated, to the extent that the client or entity is not a "Restricted Person", but may not share with or permit the client or entity to review the "HIGHLY CONFIDENTIAL PROTECTED MATERIAL." Such discussions must be general in nature and not disclose specific "HIGHLY CONFIDENTIAL PROTECTED MATERIAL."

9. Information deemed Proprietary Information shall not be used except as necessary for the conduct of these proceedings, nor shall it be disclosed in any manner to any person except a Reviewing Representative who is engaged in the conduct of these proceedings and who needs to know the information in order to carry out that person's responsibilities in these proceedings.

10. Reviewing Representatives may not use information contained in any Proprietary Information obtained through these proceedings to give any party or any competitor or customer or consignee of any party a commercial advantage. In the event that a party wishes to designate as a Reviewing Representative a person not described in Paragraphs 5(i) through 5(iv) or 6(i)

through 6(iii) above, the party shall seek agreement from the party providing the Proprietary Information. If an agreement is reached, that person shall be a Reviewing Representative pursuant to Paragraph 6(iv) above with respect to those materials. If no agreement is reached, the party shall submit the disputed designation to the presiding Administrative Law Judge for resolution.

11. (a) A Reviewing Representative shall not be permitted to inspect, participate in discussions regarding, or otherwise be permitted access to Proprietary Information pursuant to this Protective Order unless that Reviewing Representative has first executed a Non-Disclosure Certificate provided that if an attorney qualified as a Reviewing Representative has executed such a certificate, the paralegals, secretarial and clerical personnel under the attorney's instruction, supervision or control need not do so. A copy of each Non-Disclosure Certificate shall be provided to counsel for the parties asserting confidentiality prior to disclosure of any Proprietary Information to that Reviewing Representative.

(b) Attorneys and outside experts qualified as Reviewing Representatives are responsible for ensuring that persons under their supervision or control comply with the Protective Order.

12. None of the parties waive their right to pursue any other legal or equitable remedies that may be available in the event of actual or anticipated disclosure of Proprietary Information.

13. The parties shall designate data or documents as constituting or containing Proprietary Information by marking the documents "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL PROTECTED MATERIAL." Where only part of data compilations or multi-page documents constitutes or contains Proprietary Information, the parties, insofar as reasonably practicable within discovery and other time constraints imposed in these proceedings, shall designate only the specific data or pages of documents which constitute or contain Proprietary Information. The Proprietary Information shall be served upon the parties hereto only in an envelope separate from the nonproprietary materials, and the envelope shall be

conspicuously marked "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL PROTECTED MATERIAL."

14. The parties will consider and treat the Proprietary Information as within the exemptions from disclosure provided in Section 335(d) of the Public Utility Code, 66 Pa. C.S. § 335(d), and the Pennsylvania Right-to-Know Act, 65 P.S. §§ 67.101 *et seq.*, until such time as the information is found to be non-proprietary. In the event that any person or entity seeks to compel the disclosure of Proprietary Information, the non-producing party shall promptly notify the producing party in order to provide the producing party an opportunity to oppose or limit such disclosure.

15. Any public reference to Proprietary Information by a party or its Reviewing Representatives shall be to the title or exhibit reference in sufficient detail to permit persons with access to the Proprietary Information to understand fully the reference and not more. The Proprietary Information shall remain a part of the record, to the extent admitted, for all purposes of administrative or judicial review.

16. Part of any record of these proceedings containing Proprietary Information, including but not limited to all exhibits, writings, testimony, cross examination, argument, and responses to discovery, and including reference thereto as mentioned in Paragraph 15 above, shall be sealed for all purposes, including administrative and judicial review, unless such Proprietary Information is released from the restrictions of this Protective Order, either through the agreement of the parties to this proceeding or pursuant to an order of the Commission.

17. The parties shall retain the right to question or challenge the confidential or proprietary nature of Proprietary Information and to question or challenge the admissibility of Proprietary Information. If a party challenges the designation of a document or information as proprietary, the party providing the information retains the burden of demonstrating that the designation is appropriate.

18. The parties shall retain the right to question or challenge the admissibility of Proprietary Information; to object to the production of Proprietary Information on any proper

ground; and to refuse to produce Proprietary Information pending the adjudication of the objection.

19. Within 30 days after a Commission final order is entered in the above-captioned proceedings, or in the event of appeals, within thirty days after appeals are finally decided, the parties, upon request, shall either destroy or return to the parties all copies of all documents and other materials not entered into the record, including notes, which contain any Proprietary Information. In the event that a party elects to destroy all copies of documents and other materials containing Proprietary Information instead of returning the copies of documents and other materials containing Proprietary Information to the parties, the party shall certify in writing to the other producing party that the Proprietary Information has been destroyed.

Dated: _____ /s/
Elizabeth H. Barnes
Administrative Law Judge

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

MEGHAN FLYNN ROSEMARY FULLER MICHAEL WALSH NANCY HARKINS GERALD MCMULLEN CAROLINE HUGHES and MELISSA HAINES	:	
Complainants,	:	Docket No. C-2018-3006116 P-2018-3006117
v.	:	
SUNOCO PIPELINE L.P.,	:	
Respondent.	:	

AMENDED NON-DISCLOSURE CERTIFICATE

TO WHOM IT MAY CONCERN:

The undersigned is the _____ of _____ (the retaining party). The undersigned has read and understands the Protective Order deals with the treatment of Proprietary Information, and the undersigned is a (check ONE):

- € Reviewing Representative for CONFIDENTIAL information.
- € Reviewing Representative for CONFIDENTIAL, HIGHLY CONFIDENTIAL information, and EXTREMELY SENSITIVE MATERIALS.

The undersigned agrees to be bound by and comply with the terms and conditions of said Protective Order.

_____
Name

_____
Signature

_____
Address

_____
Employer

ATTACHMENT B

(Redline Protective Order)

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

MEGHAN FLYNN ROSEMARY FULLER MICHAEL WALSH NANCY HARKINS GERALD MCMULLEN CAROLINE HUGHES and MELISSA HAINES	Docket No.	C-2018-3006116 P-2018-3006117
Complainants,		
v.		
SUNOCO PIPELINE L.P.,		
Respondent.		

AMENDED PROTECTIVE ORDER

AND NOW, upon due consideration of the unopposed Motion for Amended Protective Order that was filed by Sunoco Pipeline L.P. on ~~November 27, 2018~~April 17, 2019;

IT IS ORDERED THAT:

1. The Motion is hereby granted with respect to all materials and information identified in Paragraphs 2 – 3 below that have been or will be filed with the Commission, produced in discovery, or otherwise presented during the above-captioned proceedings and all proceedings consolidated therewith.

2. The information subject to this Protective Order is all correspondence, documents, data, information, studies, methodologies and other materials, furnished in these proceedings, which are believed by the producing party to be of a proprietary or confidential nature and which are so designated by being marked "CONFIDENTIAL," ~~or~~ "HIGHLY CONFIDENTIAL PROTECTED MATERIAL~~,~~" or "EXTREMELY SENSITIVE MATERIALS." Such materials will be referred to below as "Proprietary Information." When a statement or exhibit is identified

for the record, the portions thereof that constitute Proprietary Information shall be designated as such for the record.

3. This Protective Order applies to the following categories of materials: (a) the parties may designate as "CONFIDENTIAL" those materials that customarily are treated by that party as sensitive or proprietary, which are not available to the public, and which, if disclosed freely, would subject that party or its clients to risk of competitive disadvantage or other business injury; (b) the parties may designate as "HIGHLY CONFIDENTIAL PROTECTED MATERIAL" those materials that are of such a commercially sensitive nature among the parties or of such a private, personal nature that the producing party is able to justify a heightened level of confidential protection with respect to those materials. Moreover, information subject to protection under the Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6) and PUC Regulations at 52 Pa. Code §§ 102.1-102.4 will also be designated as "HIGHLY CONFIDENTIAL PROTECTED MATERIAL"; (c) the parties may designate as "EXTREMELY SENSITIVE MATERIALS" those materials that are subject to protection under the Public Utility Confidential Security Information Disclosure Protection Act (35 P.S. §§ 2141.1 to 2141.6) and PUC Regulations at 52 Pa. Code §§ 102.1-102.4 and are of such an extremely sensitive security nature that the producing party is able to justify a heightened level of confidential protection with respect to those materials. The parties shall endeavor to limit their designation of information as HIGHLY CONFIDENTIAL PROTECTED MATERIAL and EXTREMELY SENSITIVE MATERIALS.

4. Proprietary Information shall be made available to counsel for a party, subject to the terms of this Protective Order. Such counsel shall use or disclose the Proprietary Information only for purposes of preparing or presenting evidence, cross examination, argument, or settlement in these proceedings. To the extent required for participation in these proceedings, counsel for a party may afford access to Proprietary Information subject to the conditions set forth in this Protective Order.

5. Information deemed as "CONFIDENTIAL" shall be made available to a "Reviewing Representative" who is a person that has signed a Non-Disclosure Certificate attached as Appendix A, and who is:

(i) An attorney who has entered an appearance in these proceedings for a party;

(ii) Attorneys, paralegals, and other employees associated for purposes of this case with an attorney described in Paragraph 5(i);

(iii) An expert or an employee of an expert retained by a party for the purpose of advising, preparing for or testifying in these proceedings; or

(iv) Employees or other representatives of a party appearing in these proceedings with significant responsibility for this docket.

6. Information deemed as "HIGHLY CONFIDENTIAL PROTECTED MATERIAL", may be provided to a "Reviewing Representative" who has signed a Non-Disclosure Certificate attached as Appendix A and who is:

(i) An attorney for a statutory advocate pursuant to 52 Pa. Code §1.8 or a counsel who has entered an appearance in these proceedings for a party;

(ii) An attorney, paralegal, or other employee associated for purposes of this case with an attorney described in Paragraph (i);

(iii) An outside expert or an employee of an outside expert retained by a party for the purposes of advising, preparing for or testifying in these proceedings; or

(iv) A person designated as a Reviewing Representative for purposes of HIGHLY CONFIDENTIAL PROTECTED MATERIAL, provided that a Reviewing Representative for purposes of HIGHLY CONFIDENTIAL PROTECTED MATERIAL shall not include an officer, director, stockholder, partner, or owner of any competitor of the parties, or of any shipper, customer or consignee of any affiliate of any competitor of the parties, or shipper, customer or consignee, or any employee of any such entity, if the employee's duties involve marketing or pricing responsibilities, or any responsibility for marketing or pricing with respect to the transportation or commodity sales and/or exchanges of refined petroleum products.

Provided, further, that in accordance with the provisions of Sections 5.362 and 5.365(e) of the Commission's Rules of Practice and Procedure, 52 Pa. Code §§ 5.362, 5.365(e), any party may, by subsequent objection or motion, seek further protection with respect to HIGHLY CONFIDENTIAL PROTECTED MATERIAL, including, but not limited to, total prohibition of disclosure or limitation of disclosure only to particular persons or parties.

7. Information deemed as "EXTREMELY SENSITIVE MATERIALS" may be provided to the same persons constituting Reviewing Representatives under paragraph 6 of this Order. However, such information will only be provided through in-person review at the offices of Manko, Gold, Katcher & Fox, 401 City Avenue, Suite 901, Bala Cynwyd, PA 19004, between the hours of 9AM to 5PM, Monday – Friday. Request to view such information shall be made to Diana Silva via email (dsilva@mankogold.com) at least 24-hours prior to the requested viewing session. Such review may be proctored and Reviewing Representatives are prohibited from reproducing such information in any form without the prior authorization of SPLP's counsel (including taking detailed notes or cell phone pictures). If a party determines that it is necessary to use an EXTREMELY SENSITIVE MATERIALS as part of their presentation of evidence in this proceeding, such party shall request a copy from counsel for Sunoco Pipeline L.P., which permission shall not be unreasonably withheld and subject to that party confirming it understands and will abide by the terms of this Protective Order concerning use of such materials.

~~7.~~8. For purposes of this Protective Order, a Reviewing Representative may not be a "Restricted Person."

(a) A "Restricted Person" shall mean: (i) an officer, director, stockholder, partner, or owner of any competitor of the parties or an employee of such an entity if the employee's duties involve marketing or pricing of the competitor's products or services; (ii) an officer, director, stockholder, partner, or owner of any affiliate of a competitor of the parties (including any association of competitors of the parties) or an employee of such an entity if the employee's duties involve marketing or pricing of the competitor's products or services; (iii) an officer, director, stockholder, owner or employee of a competitor of a customer of the parties if the Proprietary Information concerns a specific, identifiable customer of the parties; and (iv) an officer, director, stockholder, owner or employee of an affiliate of a competitor of a customer of the parties if the Proprietary Information concerns a specific, identifiable customer of the parties; provided, however, that no expert shall be disqualified on account of being a stockholder, partner, or owner unless that expert's interest in the business would provide a significant motive for violation of the limitations of permissible use of the Proprietary Information. For purposes of this Protective Order, stocks, partnership or other ownership interests valued at more than

$10,000 or constituting more than a 1% interest in a business establishes a significant motive for violation.

(b) If an expert for a party, another member of the expert's firm or the expert's firm generally also serves as an expert for, or as a consultant or advisor to, a Restricted Person, said expert must: (i) identify for the parties each Restricted Person and each expert or consultant; (ii) make reasonable attempts to segregate those personnel assisting in the expert's participation in this proceeding from those personnel working on behalf of a Restricted Person; and (iii) if segregation of such personnel is impractical the expert shall give to the producing party written assurances that the lack of segregation will in no way jeopardize the interests of the parties or their customers. The parties retain the right to challenge the adequacy of the written assurances that the parties' or their customers' interests will not be jeopardized. No other persons may have access to the Proprietary Information except as authorized by order of the Commission.

8. A qualified "Reviewing Representative" for "HIGHLY CONFIDENTIAL PROTECTED MATERIAL" may review and discuss "HIGHLY CONFIDENTIAL PROTECTED MATERIAL" with their client or with the entity with which they are employed or associated, to the extent that the client or entity is not a "Restricted Person", but may not share with or permit the client or entity to review the "HIGHLY CONFIDENTIAL PROTECTED MATERIAL." Such discussions must be general in nature and not disclose specific "HIGHLY CONFIDENTIAL PROTECTED MATERIAL."

9. Information deemed Proprietary Information shall not be used except as necessary for the conduct of these proceedings, nor shall it be disclosed in any manner to any person except a Reviewing Representative who is engaged in the conduct of these proceedings and who needs to know the information in order to carry out that person's responsibilities in these proceedings.

10. Reviewing Representatives may not use information contained in any Proprietary Information obtained through these proceedings to give any party or any competitor or customer or consignee of any party a commercial advantage. In the event that a party wishes to designate as a Reviewing Representative a person not described in Paragraphs 5(i) through 5(iv) or 6(i)

through 6(iii) above, the party shall seek agreement from the party providing the Proprietary Information. If an agreement is reached, that person shall be a Reviewing Representative pursuant to Paragraph 6(iv) above with respect to those materials. If no agreement is reached, the party shall submit the disputed designation to the presiding Administrative Law Judge for resolution.

11. (a) A Reviewing Representative shall not be permitted to inspect, participate in discussions regarding, or otherwise be permitted access to Proprietary Information pursuant to this Protective Order unless that Reviewing Representative has first executed a Non-Disclosure Certificate provided that if an attorney qualified as a Reviewing Representative has executed such a certificate, the paralegals, secretarial and clerical personnel under the attorney's instruction, supervision or control need not do so. A copy of each Non-Disclosure Certificate shall be provided to counsel for the parties asserting confidentiality prior to disclosure of any Proprietary Information to that Reviewing Representative.

(b) Attorneys and outside experts qualified as Reviewing Representatives are responsible for ensuring that persons under their supervision or control comply with the Protective Order.

12. None of the parties waive their right to pursue any other legal or equitable remedies that may be available in the event of actual or anticipated disclosure of Proprietary Information.

13. The parties shall designate data or documents as constituting or containing Proprietary Information by marking the documents "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL PROTECTED MATERIAL." Where only part of data compilations or multi-page documents constitutes or contains Proprietary Information, the parties, insofar as reasonably practicable within discovery and other time constraints imposed in these proceedings, shall designate only the specific data or pages of documents which constitute or contain Proprietary Information. The Proprietary Information shall be served upon the parties hereto only in an envelope separate from the nonproprietary materials, and the envelope shall be

conspicuously marked "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL PROTECTED MATERIAL."

14. The parties will consider and treat the Proprietary Information as within the exemptions from disclosure provided in Section 335(d) of the Public Utility Code, 66 Pa. C.S. § 335(d), and the Pennsylvania Right-to-Know Act, 65 P.S. §§ 67.101 *et seq.*, until such time as the information is found to be non-proprietary. In the event that any person or entity seeks to compel the disclosure of Proprietary Information, the non-producing party shall promptly notify the producing party in order to provide the producing party an opportunity to oppose or limit such disclosure.

15. Any public reference to Proprietary Information by a party or its Reviewing Representatives shall be to the title or exhibit reference in sufficient detail to permit persons with access to the Proprietary Information to understand fully the reference and not more. The Proprietary Information shall remain a part of the record, to the extent admitted, for all purposes of administrative or judicial review.

16. Part of any record of these proceedings containing Proprietary Information, including but not limited to all exhibits, writings, testimony, cross examination, argument, and responses to discovery, and including reference thereto as mentioned in Paragraph 15 above, shall be sealed for all purposes, including administrative and judicial review, unless such Proprietary Information is released from the restrictions of this Protective Order, either through the agreement of the parties to this proceeding or pursuant to an order of the Commission.

17. The parties shall retain the right to question or challenge the confidential or proprietary nature of Proprietary Information and to question or challenge the admissibility of Proprietary Information. If a party challenges the designation of a document or information as proprietary, the party providing the information retains the burden of demonstrating that the designation is appropriate.

18. The parties shall retain the right to question or challenge the admissibility of Proprietary Information; to object to the production of Proprietary Information on any proper

ground; and to refuse to produce Proprietary Information pending the adjudication of the objection.

19. Within 30 days after a Commission final order is entered in the above-captioned proceedings, or in the event of appeals, within thirty days after appeals are finally decided, the parties, upon request, shall either destroy or return to the parties all copies of all documents and other materials not entered into the record, including notes, which contain any Proprietary Information. In the event that a party elects to destroy all copies of documents and other materials containing Proprietary Information instead of returning the copies of documents and other materials containing Proprietary Information to the parties, the party shall certify in writing to the other producing party that the Proprietary Information has been destroyed.

Dated: ~~November 28, 2018~~

/s/
Elizabeth H. Barnes
Administrative Law Judge

BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION

MEGHAN FLYNN ROSEMARY FULLER MICHAEL WALSH NANCY HARKINS GERALD MCMULLEN CAROLINE HUGHES and MELISSA HAINES	:	
Complainants,	:	Docket No. C-2018-3006116 P-2018-3006117
v.	:	
SUNOCO PIPELINE L.P.,	:	
Respondent.	:	

AMENDED NON-DISCLOSURE CERTIFICATE

TO WHOM IT MAY CONCERN:

The undersigned is the _____ of _____ (the retaining party). The undersigned has read and understands the Protective Order deals with the treatment of Proprietary Information, and the undersigned is a (check ONE):

€ Reviewing Representative for CONFIDENTIAL information.

€ Reviewing Representative for CONFIDENTIAL ~~&~~, HIGHLY CONFIDENTIAL information, and EXTREMELY SENSITIVE MATERIALS.

The undersigned agrees to be bound by and comply with the terms and conditions of said Protective Order.

_____
Name

_____
Signature

_____
Address

_____
Employer

ATTACHMENT C

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.

Introduction[1]

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_amended.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 data[12] 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 beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.[45]

III. Conclusion

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

---

[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."

ATTACHMENT D

January 28, 2019
TECHREPORT 2018

2018 Cybersecurity

David G. Ries

Share this:

Security breaches are so prevalent that there is a new mantra in cybersecurity today—it's "when, not if" a law firm or other entity will suffer a breach. In an address at a major information security conference in 2012, then-FBI director Robert Mueller put it this way:

> "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Mueller's observation continues to be true today for attorneys and law firms as well as for small businesses through large global companies. There have been numerous reports for over a decade of law firm data breaches in the popular and legal press—print and online. The FBI has reported that law firms are often viewed as "one-stop shops" for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

New York Ethics Opinion 1019 warned attorneys in May 2014 about this threat environment:

> "Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks."

Several years later, ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 11, 2017), observed:

> "At the same time, the term 'cybersecurity' has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a ... world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if.' Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client."

Most recently, ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018) starts with the following observations about current threats:

> "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. 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. Indeed, the data security threat is so high that law enforcement officials regular regularly divide business entities into two categories: those that have been hacked and those that will be."

The ABA's *2018 Legal Technology Survey Report* explores security threats and incidents and safeguards that reporting attorneys and their law firms are using to protect against them. As in past years, it shows that many attorneys and law firms are employing some of the safeguards covered in the questions and generally increasing use of the safeguards over time. However, it also shows that many are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions.

Some attorneys and law firms may not be devoting more attention and resources to security because they mistakenly believe "it won't happen to me." The increasing threats to attorneys and law firms and the reports of security breaches should dispel this mistaken viewpoint. Significantly, 23% of respondents overall reported this year that their firm had experienced a data breach at some time.

Data security is addressed most directly in *2018 Survey,* "Volume I: Technology Basics & Security." It is further addressed in "Volume IV: Marketing and Communications Technology," and "Volume VI: Mobile Lawyers." This *TECHREPORT* reviews responses to the security questions in this year's Survey and discusses them in light of both attorneys' duty to safeguard information and standard information security practices. Each volume includes a Trend Report, which breaks down the information by size of firm and compares it to prior years, followed by sections with more detailed information on survey responses. This gives attorneys and law firms (and clients) information to compare their security posture to law firms of similar size.

Attorneys' Duty to Safeguard Information

The ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to clients (ABA Model Rules 1.1 and 1.6 and Comments). These duties are covered in these rules and comments and in the recent ethics opinions like the ones discussed above. Attorneys also have common law duties to protect client information and often have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information, like health and financial information. These duties present a challenge to attorneys using technology because most are not technologists and often lack training and experience in security. Compliance requires attorneys to understand limitations in their knowledge and obtain sufficient information to protect client information, to get qualified assistance if necessary, or both. These obligations are minimum standards—failure to comply with them may constitute unethical or unlawful conduct. Attorneys should aim for security that goes beyond these minimums as a matter of sound professional practice and client service.

Recognizing the Risk

Information security starts with an inventory and risk assessment to determine what needs to be protected and the threats that it faces. The inventory should include both technology and data. You can't protect it if you don't know that you have it and where it is.

Comment [18] to Model Rule 1.6 includes a risk-based approach to determine reasonable measures that attorneys should employ. The first two factors in the analysis are "the sensitivity of the information" and "the likelihood of disclosure if additional safeguards are not employed." This analysis should include a review of security incidents that an attorney or law firm has experienced and those experienced by others—generally and in the legal profession. The *2018 Survey* includes information about threats in its questions about security breaches.

The next factors in the risk analysis cover available safeguards. Comment [18] to Model Rule 1.6 includes them in the risk analysis for attorneys for determining what is reasonable:

> "...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)."

Comment [18] uses a risk-based approach that is now standard in information security. The *2018 Survey* includes information about the available safeguards that various attorneys and firms are using.

The *2018 Survey* reports that about 23% of respondents overall reported that their firms had experienced a security breach at some point. The question is not limited to the past year, it's "ever." A breach broadly includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit. This compares with 22% last year, 14% in 2016, 15% in 2015, 14% in 2014, and 15% in 2013—an increase of 8% in 2017 after being basically steady from 2013 through 2016.

This year, the reported percentage of firms experiencing a breach generally increased with firm size, ranging from 14% of solos, 24% of firms with 2-9 attorneys, about 24% for firms with 2-9 and 10-49, 42% with 50-99, and about 31% with 100+. As noted above, this is for firms who have experienced a breach *ever*, not just in the past year.

Larger firms have more people, more technology, and more data, so there is a greater exposure surface, but they also should have more resources to protect them. It is difficult to tell the completeness of larger firm's responses on breaches because the percentage of those reporting that they "don't know" about breaches (18% overall) directly goes up with firm size—reaching 57% in firms with 100-499 attorneys and 61% in firms with 500+. This makes sense because attorneys in medium and large firms may not learn about security incidents that don't impact the entire firm, particularly minor incidents and ones at remote offices.

The majority of respondents—60%—reported that their firm had not experienced a breach in the past. Hopefully, this does not include firms that have experienced a security breach and never detected it. Another common saying in security today is that there are two kinds of companies: Those that have been breached and know it, and those that have been breached but don't know it. The same is likely true for law firms.

The most serious consequence of a security breach for a law firm would most likely be unauthorized access to sensitive client data (although the loss of data would also be very serious). The *2018 Survey* shows a very low incidence of this result for firms that experienced a breach—about 6% overall, up from 1% last year. The reports of unauthorized access to sensitive client data by firms that experienced a breach is 11% for solos (up from none last year); 6-8% for firms with 2-9, 10-49, and 50-99; none reported for firms with 100+. While the percentages are low, any exposure of client data can be a major disaster for a law firm and its clients.

The information on breaches with exposure of client data is incomplete because almost 7% overall report that they don't know about the consequences, with "don't know" responses increasing from none for solos to 38% for firms of 500+. The uncertainty is increased by the high percentage of respondents (18%), discussed above, who don't even know whether their firm experienced a data breach.

Unauthorized access to non-client sensitive data is 6% overall, with 8% for solos, 5% for firms with 2-9, 10% for firms with 10-49, 8% for firms with 50-99, 5% for firms of 100-499, and none for firms with 500+.

The other reported consequences of data breaches are significant. Downtime/loss of billable hours was reported by 41% of respondents; consulting fees for repair were reported by 40%; destruction or loss of files by 11%, and replacement of hardware/software reported by 27% (percentages for firms that experienced breaches). Any of these could be very serious, particularly for solos and small firms that may have limited resources to recover. No significant business disruption or loss was reported by 65% overall.

About 9% overall responded that they notified a client or clients of the breach. The percentage reporting notice to clients ranges from 11% for solos, 8% for firms with 2-9, 7% for firms with 10-49, 17% for firms with 50-99, none for firms with 100-499 and 19% for firms with 500+. This is equal to or in excess of the reported incidence of unauthorized access to client data for firms of each size, consistent with the view that ethical and common law obligations require notice to clients.

Overall, 14% of respondents that experienced a breach reported that they gave notice to law enforcement, ranging from 13% for solos, 10% with 2-9 attorneys, 20% of firms with 10-49, 25% of firms with 50-99, 5% of firms with 100-499 attorneys to 25% of firms with 500+.

The *2018 Survey* also inquired whether respondents ever experienced an infection with viruses/spyware/malware. Overall, 40% reported infections, 37% reported none, and 23% reported that they don't know. Reported infections were greatest in firms with 10-49 attorneys (57%) and 2-9 (48%), and lowest in firms with 500+ (20%). Infections can cause serious consequences, including compromise of confidentiality and loss of data. With over one third of respondents reporting infections (down from almost half last year), strong safeguards to protect against them, including up to date security software, using current versions of operating systems and software, promptly applying patches to the operating system and all application software, effective backup, and training of attorneys and staff are clearly warranted.

Security Programs and Policies

At the ABA Annual Meeting in August, 2014, the ABA adopted a resolution on cybersecurity that "encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected." The organizations covered by it include law firms.

A security program should address people, policies and procedures, and technology. All three areas are necessary for an effective program. Security should not be left solely to IT staff and tech consultants. In addition to measures to prevent security incidents and breaches, there has been a growing recognition that security includes the full spectrum of measures to identify and protect information assets and to detect, respond to, and recover from data breaches and security incidents. Security programs should cover all of these functions.

An important initial step in establishing an information security program is defining responsibility for security. The program should designate an individual or individuals responsible for coordinating security—someone must be in charge. It should also define everyone's responsibility for security, from the managing partner or CEO to support staff.

While a dedicated, full-time Chief Information Security Officer is generally only appropriate (and affordable) for larger law firms, every firm should have someone who is responsible for coordinating security. The larger the firm, the more necessary it is to have a full-time security officer or someone who is to dedicate an appropriate part of their time and effort to security. The *2018 Survey* asks who has primary responsibility for security in respondents' firms. As expected, responses vary by size of firm. The respondent has primary responsibility in solo firms (84%), the

respondent or an external consultant/expert in firms of 2-9 attorneys (27% and 33%, respectively); IT staff for firms of 10-49 attorneys (41%) and 50-99 (47%), a chief information officer in firms of 100-499 (56%) and firms of 500+ (62%). A small percentage (2%) report that nobody has primary responsibility for security—a high-risk situation.

The *2018 Survey* asks respondents about a variety of technology-related policies, rather than about an overall comprehensive information security program. Attorneys and law firms should view these kinds of policies as part of a coordinated program rather than individually.

According to the *2018 Survey*, 53% of respondents report that their firms have a policy to manage the retention of information/data held by the firm, 50% report a policy on email use, 44% for internet use, 41% for computer acceptable use, 37% remote access, 38% for social media, 21% personal technology use/BYOD, and 32% for employee privacy. The numbers generally increase with firm size. For example, about 33% of solo respondents report having an information/data retention policy, increasing to 51% in firms with 2-9, 60% with 10-49, 77% with 50-99, and approximately 90% in 100+ attorneys.

Two responses that raise a major security concern are those that report having no policies (29% overall) and those reporting that they don't know about security policies (7%). There is a clear trend by firm size in the responses of having no policies. There are no respondents in firms of 100+ attorneys reporting none. The percentage with none generally decreases by firm size, ranging from 3% of firms with 50-99, 6% with 10-49, 25% in firms with 2-9, to 58% of responding solos. While it is understandable that solos and smaller firms may not appreciate the need for policies, all firms should have policies, appropriately scaled to the size of the firm and the sensitivity of the data.

Incident response is a critical element of an information security program. Overall, 25% report having an incident response plan. The percentage of respondents reporting that they have incident response plans varies with firm size, ranging from 9% for solos and 16% for firms with 2-9 to approximately 70% forms with 100+. As with a comprehensive security program, all attorneys and law firms should have an incident response plan scaled to the size of the firm. For solos and small firms, it may just be a checklist plus who to call for what, but they should have a basic plan.

Security awareness is a key to effective security. There cannot be effective security if users are not trained and do not understand the threats, how to protect against them, and the applicable

security policies. Obviously, they can't understand policies if they don't even know whether their law firm has any policies.

In accordance with the ABA resolution on cybersecurity programs (and generally accepted security practices), all attorneys and law firms should have security programs tailored to the size of the firm and the data and systems to be protected. They should include training and constant security awareness.

Security Assessments and Client Requirements

Clients are increasingly focusing on the information security of law firms representing them and using approaches like required third-party security assessments, security requirements, and questionnaires.

The increased use of security assessments conducted by independent third parties has been a growing security practice for businesses and enterprises generally. Law firms have been slow to adopt this security tool, with only 28% of law firms overall reporting that they had a full assessment, but it increased from 27% last year and 18% in 2017. Affirmative responses generally increase by size of firm.

Third-party assessments are often conducted for law firms only when a client requests it or requires it. Overall, 11% report that a client or prospective client has requested an audit or other review. The percentage of firms reporting a client request gradually goes up by size of firm, from 2% for solos to 39% for firms of 500+.

Overall, 34% of respondents report that they have received a client security requirements document or guidelines. Firms receiving them generally increase by size of firm, from 15% of solos to about 66% with 100+ attorneys. There is a growing recognition in the information security profession of the importance of securing data that business partners and service providers can access, process, and store. This includes law firms. In March of 2017, the Association of Corporate Counsel (ACC) published the *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information* that provides a list of baseline security measures and controls that legal departments can consider in developing requirements for outside counsel. Attorneys and law firms are likely to continue to face increasing client requirements for security.

Cyber Insurance

As the headlines continue to be filled with reports of data breaches, including law firms, there has been a growing recognition of the need for cyber insurance. Many general liability and malpractice policies do not cover security incidents or data breaches. The percentage of attorneys reporting that they have cyber liability coverage is small but has been increasing—34% overall (up from 27% in 2017, 17% in 2016, and 11% in 2015). It gradually increases from 27% for solos to about 35-45% for midsize firms, then drops to 23% for firms of 500+. In addition to cyber liability insurance, covering liability to third parties, there is also coverage available for first-party losses to the law firm (like lost productivity, data restoration, and technical and legal expenses). A review of the need for cyber insurance coverage should be a part of the risk assessment process for law firms of all sizes.

Security Standards and Frameworks

A growing number of law firms are using information security standards and frameworks, like those published by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS). They provide consensus approaches to a comprehensive information security program. Some firms use them as guidelines for their security programs, while a smaller group of firms seek formal security certification. The *2018 Survey* asks whether respondents' firms have received a security certification. Overall, only 9% report that they have received certification, with a low of 3% for solos and a high of 27% for firms with 500+.

Authentication and Access Control

Authentication and access controls are the first lines of defense. They are the "keys to the kingdom"—controlling access to networks, computers, and mobile devices.

The *2018 Survey* includes a general question about mandatory passwords without specifying the access for which they are required. Overall, 68% of respondents report using mandatory passwords. They are required by 53% of solos, 71% of firms of 2-10 attorneys, and about 80% or higher for larger firms. This question does not ask about other forms of authentication like fingerprints or facial recognition. Some form of strong authentication should be required for access to computers and networks for all attorneys and all law firms.

For laptops, a strong majority of responding attorneys—nearly all—report that they use access controls. Overall, 98% report using passwords, with 99% for solos, 98% for firms of 2-9 attorneys, 94% for firms of 10-49, and firms of 50-500+ at 100%. In addition, 19% overall report using other authentication, which would include fingerprint readers, facial recognition, and other alternatives. While this might suggest that all attorneys use some form of access control (98% + 19%), that is not the case. About 1% report that they use none of the listed laptop security measures. The response of "none" only includes solos and firms 10-49 attorneys. As noted above, larger firms report 100% use of passwords for laptops.

Use of authentication controls on smartphones is similar to those on laptops. Reported use of passwords is 92% overall—generally increasing with firm size from 87% for solos to 100% for firms of 500+. Firms of other sizes range from about 90% to 99%. Use of other authentication is 40% overall, while 5% reporting none of the listed security measures.

For both laptops and smartphones (as well as other mobile and portable devices), all attorneys should be using strong passwords or other strong authentication.

Most, if not all, attorneys need multiple passwords for a number of devices, networks, services, and websites—for both work and personal use. It is recommended that users have a different, strong password for each device, network, service, and website. While password standards are evolving—stressing length over complexity—it is very difficult, or impossible, to remember numerous passwords. Password management tools allow a user to remember a single, strong password for the tool or locker with automatic access to the others. Respondents report that 24% overall use password management tools. 16% report that they don't know. It is unlikely that respondents who don't know are using these tools because a user would have to know that they are using a single password to access others. There is some difference in use by size of firm, ranging from a low of 16% for firms with 50-99 attorneys to a high of 30% for firms with 100-499.

Encryption

Encryption is a strong security measure that protects data in storage (on computers, laptops, smartphones, tablets, and portable devices) and transmitted data (over wired and wireless networks, including email). Security professionals view encryption as a basic safeguard that should be widely deployed. It is increasingly being required by law for personal information, like health and financial information. The recent battle between the FBI and Apple and the current debate about mandated "backdoors" to encryption for law enforcement and national security

show how strong encryption can be for protecting sensitive data. The *2018 Survey* shows that use by attorneys of the covered encryption tools has been growing, but its use is limited.

Full-drive encryption provides strong protection for all of the data on a server, desktop, laptop, or portable device. The data is readable only when it is decrypted through use of the correct password or other access control. Respondents report an overall use of full-drive encryption of only 24% (up from 21% last year and 15% in 2016), ranging from 15% for solos to about 48% for firms of 100+, with percentages increasing by firm size. File encryption protects individual files rather than all the data on a drive or device. Reported use of file encryption is higher than full disk at 46% overall, ranging from 36% for solos to 72% in firms of 500+. This question is general and is not broken down in Volume I of the *2018 Survey* by servers, desktops, laptops, smartphones, etc. As discussed below, all attorneys should use encryption on laptops, smartphones, and mobile devices. While some law firms are starting to encrypt desktops and firm servers, it is not yet a common practice.

Volume VI of the *2018 Survey* has separate questions for laptops and smartphones. For laptops, 25% overall report using file/data encryption and 18% report using hard drive encryption. Both of these numbers are down slightly from last year. File/data protection relies on the user to encrypt individual files or to put sensitive information in an encrypted file or partition on the drive. Full-drive encryption provides broader protection because it protects all data on the drive. Use of full-drive encryption for laptops does not vary directly with firm size—reported use is 18% for solos, 13% for firms with 2-9, 26% for firms with 10-49, 18% of firms with 50-99, 30% of firms with 100-499, and only 15% of firms with 500+ attorneys.

The *2018 Survey* also reported on additional security measures for laptops, like remote data wiping (12% overall) and tracking software (7% overall). These kinds of measures can provide additional security, but should not be a substitute for strong authentication and encryption.

Use of encryption on smartphones appears to be significantly under-reported by attorneys responding to the *2018 Survey*, as in past years. Respondents report an overall use of encryption of smartphones by only 18%. However, 72% overall of attorneys who use smartphones for work report using iPhones and 94% report that they use password protection on their smartphones. On current iPhones, encryption is automatically enabled when a PIN or passcode is set. Google is also moving to automatic encryption with a PIN or swipe pattern for Android devices. It appears that many attorneys are using encryption on their smartphones without knowing it. Encryption can

be that easy! Encryption of laptops may also be under-reported because it can be transparent to the user if it has been enabled or installed by a law firm's IT staff or a technology consultant.

Verizon's *2014 Data Breach Investigation Report* concludes that "encryption is as close to a no-brainer solution as it gets" for lost or stolen devices. Attorneys who do not use encryption on laptops, smartphones, and portable devices should consider the question: Is failure to employ what many consider to be a no-brainer solution taking competent and reasonable measures?

Secure email is another safeguard with limited reported use by responding attorneys. Overall, 29% of respondents reported that they use encryption of email for confidential/privileged communications/documents sent to clients (down from 36% last year). This ranges from 19% for solos, gradually increasing to 70% with firms of 50-99 and 73% for firms of 500+. Firms of 100-499 are an exception, with only 47% reporting use of encryption for email. Another question asks about registered/secure email, which appears to also include encryption. Overall, 18% report using registered/secure email, increasing directly with firm size from 12% for solos to 36% for firms with 500+. If there is no overlap between this response and the use of encryption, the overall percentage using email security would be 47% overall, increasing with firm size to 100% of firms with 500+.

Email encryption has now become easy to use and inexpensive with commercial email services. Google and Yahoo, at least in part driven by the disclosures about NSA interception, announced in 2014 that they would be making encryption available for their email services. In its announcement, Google compared unencrypted email to a postcard and encryption as adding an envelope. This postcard analogy has been used by security professionals for years. Hopefully, the percentages of attorneys reporting that they have added the envelopes, where appropriate, will grow in future survey results.

During the last several years, some state ethics opinions have increasingly expressed the view that encryption of email may sometimes be required to comply with attorneys' duty of confidentiality. On May 11, 2017, the ABA issued Formal Opinion 477, Securing Communication of Protected Client Information. The Opinion revisits attorneys' duty to use encryption and other safeguards to protect email and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and concludes "the use of un-encrypted routine email generally remains an acceptable method of lawyer-client communication," but "particularly strong protective measures, like encryption, are warranted in some circumstances." It notes that attorneys are required to use special security precautions, like encryption, "when

required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

If encrypted email is not available, a strong level of protection can be provided by putting the sensitive information in an encrypted attachment instead of in the text of the email. In current versions of Microsoft Office, Adobe Acrobat, and WinZip, setting a password for the document encrypts it. While password protection of documents is not as strong as encryption of a complete email and attachments because it depends on the strength of the password, it is much more secure than no encryption. If this approach is used, it is important to securely provide the passwords or passphrase to the recipient(s), preferably through a different communication channel like a phone call or text message (and certainly not in the email used to send the document).

Overall, a low percentage of respondents report using password protection for documents. There is not a pattern by firm size, with a low of 12% reported by solos and a high of 35% reported by firms of 100-499.

It has now reached the point where all attorneys should generally understand encryption and have encryption available for use in appropriate circumstances.

Some Basic Security Tools

In addition to authentication and encryption, the *2018 Survey* asks about various security tools that are available to responding attorneys. Most, if not all, of these tools are security basics that should be used by all attorneys and law firms.

The most common tool is the spam filter, used by 87% of respondents. This may be under-reported because most email service providers have at least basic spam filters. Spam filters can be a strong first line of defense against phishing (malicious emails that try to steal information or plant malware). Filters are only part of the defense that weeds out some phishing emails but are an important first step.

Other tools with high reported use include anti-spyware (80%), software-based firewalls (80%), antivirus for desktops/laptops (73%), for email (69%), for networks (66%), and hardware firewalls (57%). Use of intrusion detection and prevention systems is reported by about 33% of respondents overall. There has been a growing trend for a number of years to use security suites that combine

some of these tools like malware protection, spyware protection, software firewalls, and basic intrusion protection in a single tool. Availability of the various security tools is generally stable across firms of all sizes, with increases for some of them with the size of the firm. For all of these security tools, the use by firms should be 100%. There is a generally low incidence of "don't know" responses for these tools, about 7% overall.

Remote Access

Approximately 90% of respondents reported that they remotely access work assets other than email, like applications and files, consistent with today's mobile practice of law. 39% report regular use of remote access, 31% report occasional use, and 19% report "seldom." Reported use generally increases with firm size, reaching 68% for firms of 500+. Respondents report using the following security measures: web-based applications (42%), virtual private networks (VPNs) (37%), remote access software (30%), and other (10%). Security for remote access is critical because it can provide unauthorized access for outsiders (to the communication or network) if it is not properly secured with an encrypted communication connection and strong authentication. There is a growing practice of using multifactor authentication or two-step verification for authentication in remote access. It requires a second method of authentication, in addition to a password, like a set of numbers transmitted to a smartphone or generated by an app. Multiple inexpensive and easy-to-use options are available.

Wireless Networks

Public wireless (WiFi) networks present a high-security risk, particularly if they are open, as in not requiring a password for connection. Without appropriate security measures, others connected to the network—both authorized users and attackers—may be able to intercept or view data and electronic communications transmitted over the network. The *2018 Survey* asks about security measures that attorneys use when accessing public wireless networks. 31% report that they do not use public wireless networks. Overall, 38% report that they use a VPN (a technology that provides an encrypted connection over the internet or other networks), 20% report that they use remote access software, 15% report that they use website-provided SSL/HTTPS encryption, and 0.6% report using other security measures. The remaining 15% are living dangerously, reporting that they use none of the security measures.

Cell carriers' data networks generally provide stronger security than public WiFi, either with access built into a smartphone, tablet, or laptop, or by using a smartphone, tablet, or separate

device as a personal hotspot.

Up-to-date equipment and secure configuration (using encryption) are also important for a law firm and home wireless networks.

Disaster Recovery/Business Continuity

Threats to the availability of data can range from failure of a single piece of equipment to a major disaster like a fire or hurricane. An increasing threat to attorneys and law firms of all sizes is ransomware, generally spread through phishing. It encrypts a user's or network's data and demands ransom (to be paid by Bitcoin) for release of the decryption key. Effective backup, which is isolated from production networks, can provide timely recovery from ransomware.

Overall, 17% of respondents report that their firm had experienced a natural or man-made disaster, like a fire or flood. The highest incidence, about 32%, was in firms of 50-99 and 500+. The lowest reported incidence was for solos at 10%, with the rest were between these numbers. Disasters of this kind can put a firm out of business temporarily or permanently. These positive responses, from 10% to 32% of respondents, and the potentially devastating results demonstrate the importance for law firms of all sizes to be prepared to respond and recover.

Despite this clear need, only 40% overall of responding attorneys report that their firms have a disaster recovery/business continuity plan. Firms with a plan generally increase with the size of the firm, ranging from 22% of solos to over 85% of firms with 50-99 and 500+ attorneys. As with comprehensive security programs, all law firms should have a disaster recovery/business continuity plan, appropriately scaled to its size.

In the equipment failure area, 34% of respondents reported that their firm experienced a hard drive failure, while 44% reported that they did not. The remainder reported that they do not know, with the "don't knows" increasing by firm size. In firms of 500+, 73% responded that they don't know. In firms of 100-499, it was 61%. It is very likely that most large firms have suffered multiple hard drive failures, just not known by the individual responding attorneys. Even limiting the analysis to known hard drive failures, they have impacted about one-third of respondents. That's a high risk, particularly considering the potential consequences of lost data, and all attorneys and law firms should implement backup and recovery measures.

Backup of data is critical for business continuity, particularly with the current epidemic of ransomware. Fortunately, most firms report that they employ some form of backup. Only 1.5% report that they don't back up their computer files. 21% of respondents report that they don't know about backup. The most frequently reported form of backup is external hard drives (38%), followed by offsite backup (30%), online backup (30%), network attached storage (15%), USB (9%), tape (7%), RAID (7%), CDs (4%), and DVDs (4%).

The *2018 Survey* responses show that 49% of respondents back up once a day, 22% more than once a day, 11% weekly, 5% monthly, and 2% quarterly. 8% report that they don't know, with unknowns increasing with firm size. Attorneys and firms that don't back up on a daily basis, or more frequently, should reevaluate the risk in light of ransomware, hardware failures, disasters, and other incidents reported in the *2018 Survey*.

Conclusion

The *2018 Survey* provides a good overview, with supporting details, of what attorneys and law firms are doing to protect confidential information. Like the last several years, the data generally shows increasing attention to security and increasing use of the covered safeguards but also demonstrates that there is still a lot of room for improvement. Attorneys and law firms who are behind the reporting attorneys and firms on safeguards should evaluate their security posture to determine whether they need to do more to provide, at minimum, competent and reasonable safeguards—and hopefully more. Those who are in the majority on safeguards, or ahead of the curve, still need to review and update their security as new technology, threats, and available safeguards evolve over time. Effective security is an ongoing process, not just a "set it and forget it" effort. All attorneys and law firms should have appropriate comprehensive, risk-based security programs that include appropriate safeguards, training, periodic review and updating, and constant security awareness.

Authors

ENTITY:

LAW PRACTICE DIVISION, LEGAL TECHNOLOGY RESOURCE CENTER

TOPIC:

CYBERSECURITY, TECHNOLOGY

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a true copy of the forgoing document upon the parties, listed below, in accordance with the requirements of § 1.54 (relating to service by a party). This document has been filed electronically on the Commission's electronic filing system and served on the following:

VIA ELECTRONIC AND FIRST CLASS

Michael S. Bomstein, Esquire
Pinnola & Bomstein
Suite 2126 Land Title Building
100 South Broad Street
Philadelphia, PA 19110
mbomstein@gmail.com

Counsel for Complainants

Rich Raiders, Esquire
Raiders Law
321 East Main Street
Annville, PA 17003
rich@raiderslaw.com

Counsel for Andover Homeowner's Association, Inc.

Anthony D. Kanagy, Esquire
Garrett P. Lent, Esquire
Post & Schell PC
17 North Second Street, 12th Floor
akanagy@postschell.com
glent@postschell.com

Counsel for Range Resources – Appalachia LLC

Margaret A. Morris, Esquire
Reger Rizzo & Darnall LLP
Cira Centre, 13th Floor
2929 Arch Street
Philadelphia, PA 19104
mmorris@regerlaw.com

Counsel for East Goshen Township, and Chester County, Pennsylvania

Guy A. Donatelli, Esquire
Lamb McErlane, PC
24 East Market St., Box 565
West Chester, PA 19382-0565
gdonatelli@lambmcerlane.com

Counsel for Downingtown Area School District, Chester County, Pennsylvania and Rose Tree Media School District, Delaware County, Pennsylvania

Leah Rotenberg, Esquire
Mays, Connard & Rotenberg LLP
1235 Penn Avenue, Suite 202
Wyomissing, PA 19610
rotenberg@mcr-attorneys.com

Counsel for Twin Valley School District, Berks County, Pennsylvania

Vincent M. Pompo, Esquire
Lamb McErlane, PC
24 East Market St., Box 565
West Chester, PA 19382-0565
vpompo@lambmcerlane.com

Counsel for West Whiteland Township, Chester County, Pennsylvania

Alex J. Baumler, Esquire
Lamb McErlane, PC
24 East Market St., Box 565
West Chester, PA 19382-0565
abaumler@lambmcerlane.com

Counsel for Downingtown Area School District, Chester County, Pennsylvania, Rose Tree Media School District, Delaware County, Pennsylvania, and West Whiteland Township

Mark L. Freed
Curtin & Heefner LP
2005 S. Easton Road, Suite 100
Doylestown, PA 18901
mlf@curtinheefner.com

Counsel for Uwchlan Township

James R. Flandreau, Esquire
Paul, Flandreau & Berger, LLP
320 W. Front Street
Media, PA 19063
jflandreau@pfblaw.com

Counsel for Middletown Township

Michael Maddren, Esquire
Patricia Sons Biswanger, Esquire
Office of the Solicitor
County of Delaware
Government Center Building
201 West Front Street
Media, PA 19063
MaddrenM@co.delaware.pa.us
patbiswanger@gmail.com

Counsel for County of Delaware

James C. Dalton, Esquire
Unruh Turner Burke & Frees
P.O. Box 515
West Chester, PA 19381-0515
jdalton@utbf.com

Counsel for West Chester Area School District, Chester County, Pennsylvania

Thomas J. Sniscak

Thomas J. Sniscak, Esq.
Kevin J. McKeon, Esq.
Whitney E. Snyder, Esq.

Dated: April 17, 2019