

Ethical Considerations and Duties in Cyber Security: The Risks You Must Know, the Strategies You Cannot Avoid

**Presented By:
Devika Kewalramani, Esq.**



**Ethical Obligations in Cyber
Security:
The Risks You Must Know, The
Responsibilities You Cannot Avoid**

July 14, 2018

Presented By:
Devika Kewalramani, Esq.
Partner, Moses & Singer LLP

***Ethical Obligations in Cyber Security:
The Risks You Must Know, The Responsibilities You Cannot Avoid***

July 14, 2018

Presented By: Devika Kewalramani, Esq.

TABLE OF CONTENTS

1. The New York Rules of Professional Conduct:
 - Rule 1.1 – Competence; Comment [8]
 - Rule 1.4 – Communication
 - Rule 1.6 – Confidentiality of Information; Comment [17]
 - Rule 5.1 – Responsibilities of Law Firms, Partners, managers and Supervisory Lawyers
 - Rule 5.3 – Lawyer’s Responsibility for Conduct of Nonlawyers; Comments [2] & [3]
2. American Bar Association Model Rules of Professional Conduct,
https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html [See link - not included]
3. Ethics Opinions:
 - N.Y. State Bar Association Ethics Opinion 842 (2010) – Using an outside online cloud storage provider to store client confidential information.
 - N.Y. State Bar Association Ethics Opinion 1019 (2014) – Confidentiality; Remote Access to Firm’s Electronic Files.
 - N.Y. State Bar Association Ethics Opinion 1020 (2014) – Confidentiality; use of cloud storage for purposes of a transaction.

N.Y. City Bar Opinion 2015-3 (2015) – Lawyers who fall victim to internet scams.

The State Bar of California Formal Opinion No. 2010-179 (2010) –
[http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4\\$3d&tabid=836](http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4$3d&tabid=836) [See link - not included]

American Bar Association Formal Opinion 477 (2017) – Securing Communication of Protected Client Information.
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf [See link - not included]

4. Cases of Interest:

Robert Millard and Bethany Millard v. Patricia L. Doran, Esq.,
Index No: 153262/2016, Supreme Court, New York County (April 18, 2016)
[not included]

Jason Shore and Coinabul, LLC v. Johnson & Bell, Ltd.
SDNY, 16 cv 4363 (April 15, 2016) [not included]

5. Speaker “bio”

* * *

**RULE 1.1:
COMPETENCE**

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) A lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

Comment

Retaining or Contracting with Lawyers Outside the Firm

[8] To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.

**RULE 1.4:
COMMUNICATION**

(a) A lawyer shall:

(1) promptly inform the client of:

(i) any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(j), is required by these Rules;

(ii) any information required by court rule or other law to be communicated to a client; and

(iii) material developments in the matter including settlement or plea offers.

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with a client's reasonable requests for information;
and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by these Rules or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

RULE 1.6:
CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

- (1) the client gives informed consent, as defined in Rule 1.0(j);
- (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or
- (3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

- (1) to prevent reasonably certain death or substantial bodily harm;
- (2) to prevent the client from committing a crime;
- (3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;
- (4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;
- (5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or
(ii) to establish or collect a fee; or
- (6) when permitted or required under these Rules or to comply with other law or court order.

(c) A lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client, except that a lawyer may reveal the information permitted to be disclosed by paragraph (b) through an employee.

Comment

Duty to Preserve Confidentiality

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

**RULE 5.1:
RESPONSIBILITIES OF LAW FIRMS, PARTNERS, MANAGERS AND SUPERVISORY
LAWYERS**

(a) A law firm shall make reasonable efforts to ensure that all lawyers in the firm conform to these Rules.

(b) (1) A lawyer with management responsibility in a law firm shall make reasonable efforts to ensure that other lawyers in the law firm conform to these Rules.

(2) A lawyer with direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the supervised lawyer conforms to these Rules.

(c) A law firm shall ensure that the work of partners and associates is adequately supervised, as appropriate. A lawyer with direct supervisory authority over another lawyer shall adequately supervise the work of the other lawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter, and the likelihood that ethical problems might arise in the course of working on the matter.

(d) A lawyer shall be responsible for a violation of these Rules by another lawyer if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the other lawyer practices or is a lawyer who has supervisory authority over the other lawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

**RULE 5.3:
LAWYER'S RESPONSIBILITY FOR CONDUCT OF NONLAWYERS**

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the nonlawyer is employed or is a lawyer who has supervisory authority over the nonlawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

Comment

[2] With regard to nonlawyers, who are not themselves subject to these Rules, the purpose of the supervision is to give reasonable assurance that the conduct of all nonlawyers employed by or retained by or associated with the law firm, including nonlawyers outside the firm working on firm matters, is compatible with the professional obligations of the lawyers and firm. Lawyers typically employ nonlawyer assistants in their practice, including secretaries, investigators, law student interns and paraprofessionals. Such nonlawyer assistants, whether they are employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. Likewise, lawyers may employ nonlawyers outside the firm to assist in

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include (i) retaining or contracting with an investigative or paraprofessional service, (ii) hiring a document management company to create and maintain a database for complex litigation, (iii) sending client documents to a third party for printing or scanning, and (iv) using an Internet-based service to store client information. When using such services outside the firm, a lawyer or law firm must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm. The extent of the reasonable efforts required under this Rule will depend

upon the circumstances, including: (a) the education, experience and reputation of the nonlawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; (f) whether the client will be supervising all or part of the nonlawyer's work. *See also* Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4 (professional independence of the lawyer) and 5.5 (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.



NEW YORK STATE BAR ASSOCIATION
Serving the legal profession and the community since 1876

ETHICS OPINION 842

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Rules: 1.4, 1.6(a), 1.6(c)

QUESTION

1. MAY A LAWYER USE AN ONLINE SYSTEM TO STORE A CLIENT'S CONFIDENTIAL INFORMATION WITHOUT VIOLATING THE DUTY OF CONFIDENTIALITY OR ANY OTHER DUTY? IF SO, WHAT STEPS SHOULD THE LAWYER TAKE TO ENSURE THAT THE INFORMATION IS SUFFICIENTLY SECURE?

OPINION

2. VARIOUS COMPANIES OFFER ONLINE COMPUTER DATA STORAGE SYSTEMS THAT ARE MAINTAINED ON AN ARRAY OF INTERNET SERVERS LOCATED AROUND THE WORLD. (THE ARRAY OF INTERNET SERVERS THAT STORE THE DATA IS OFTEN CALLED THE "CLOUD.") A SOLO PRACTITIONER WOULD LIKE TO USE ONE OF THESE ONLINE "CLOUD" COMPUTER DATA STORAGE SYSTEMS TO STORE CLIENT CONFIDENTIAL INFORMATION. THE LAWYER'S AIM IS TO ENSURE THAT HIS CLIENTS' INFORMATION WILL NOT BE LOST IF SOMETHING HAPPENS TO THE LAWYER'S OWN COMPUTERS. THE ONLINE DATA STORAGE SYSTEM IS PASSWORD-PROTECTED AND THE DATA STORED IN THE ONLINE SYSTEM IS ENCRYPTED.

3. A DISCUSSION OF CONFIDENTIAL INFORMATION IMPLICATES RULE 1.6 OF THE NEW YORK RULES OF PROFESSIONAL CONDUCT (THE "RULES"), THE GENERAL RULE GOVERNING CONFIDENTIALITY. RULE 1.6(A) PROVIDES AS FOLLOWS:

A LAWYER SHALL NOT KNOWINGLY REVEAL CONFIDENTIAL INFORMATION . . . OR USE SUCH INFORMATION TO THE DISADVANTAGE OF A CLIENT OR FOR THE ADVANTAGE OF A LAWYER OR A THIRD PERSON, UNLESS:

- (1) THE CLIENT GIVES INFORMED CONSENT, AS DEFINED IN RULE 1.0(d);**
- (2) THE DISCLOSURE IS IMPLIEDLY AUTHORIZED TO ADVANCE THE BEST INTERESTS OF THE CLIENT AND IS EITHER REASONABLE UNDER THE CIRCUMSTANCES OR CUSTOMARY IN THE PROFESSIONAL COMMUNITY; OR**
- (3) THE DISCLOSURE IS PERMITTED BY PARAGRAPH (b).**

4. THE OBLIGATION TO PRESERVE CLIENT CONFIDENTIAL INFORMATION EXTENDS BEYOND MERELY PROHIBITING AN ATTORNEY FROM REVEALING CONFIDENTIAL INFORMATION WITHOUT CLIENT CONSENT. A LAWYER MUST ALSO TAKE REASONABLE CARE TO AFFIRMATIVELY PROTECT A CLIENT'S CONFIDENTIAL INFORMATION. *SEEN.Y. COUNTY 733 (2004)* (AN ATTORNEY "MUST DILIGENTLY PRESERVE THE CLIENT'S CONFIDENCES, WHETHER REDUCED TO DIGITAL FORMAT, PAPER, OR OTHERWISE"). AS A NEW JERSEY ETHICS COMMITTEE OBSERVED, EVEN WHEN A LAWYER WANTS A CLOSED CLIENT FILE TO BE DESTROYED, "[S]IMPLY PLACING THE FILES IN THE TRASH WOULD NOT SUFFICE. APPROPRIATE STEPS MUST BE TAKEN TO ENSURE THAT

CONFIDENTIAL AND PRIVILEGED INFORMATION REMAINS PROTECTED AND NOT AVAILABLE TO THIRD PARTIES." NEW JERSEY OPINION (2006), QUOTING NEW JERSEY OPINION 692 (2002).

5. IN ADDITION, RULE 1.6(C) PROVIDES THAT AN ATTORNEY MUST "EXERCISE REASONABLE CARE TO PREVENT ... OTHERS WHOSE SERVICES ARE UTILIZED BY THE LAWYER FROM DISCLOSING OR USING CONFIDENTIAL INFORMATION OF A CLIENT" EXCEPT TO THE EXTENT DISCLOSURE IS PERMITTED BY RULE 1.6(B). ACCORDINGLY, A LAWYER MUST TAKE REASONABLE AFFIRMATIVE STEPS TO GUARD AGAINST THE RISK OF INADVERTENT DISCLOSURE BY OTHERS WHO ARE WORKING UNDER THE ATTORNEY'S SUPERVISION OR WHO HAVE BEEN RETAINED BY THE ATTORNEY TO ASSIST IN PROVIDING SERVICES TO THE CLIENT. WE NOTE, HOWEVER, THAT EXERCISING "REASONABLE CARE" UNDER RULE 1.6 DOES NOT MEAN THAT THE LAWYER GUARANTEES THAT THE INFORMATION IS SECURE FROM ANY UNAUTHORIZED ACCESS.

6. TO DATE, NO NEW YORK ETHICS OPINION HAS ADDRESSED THE ETHICS OF STORING CONFIDENTIAL INFORMATION ONLINE. HOWEVER, IN N.Y. STATE 709 (1998) THIS COMMITTEE ADDRESSED THE DUTY TO PRESERVE A CLIENT'S CONFIDENTIAL INFORMATION WHEN TRANSMITTING SUCH INFORMATION ELECTRONICALLY. OPINION 709 CONCLUDED THAT LAWYERS MAY TRANSMIT CONFIDENTIAL INFORMATION BY E-MAIL, BUT CAUTIONED THAT "LAWYERS MUST ALWAYS ACT REASONABLY IN CHOOSING TO USE E-MAIL FOR CONFIDENTIAL COMMUNICATIONS." THE COMMITTEE ALSO WARNED THAT THE EXERCISE OF REASONABLE CARE MAY DIFFER FROM ONE CASE TO THE NEXT. ACCORDINGLY, WHEN A LAWYER IS ON NOTICE THAT THE CONFIDENTIAL INFORMATION BEING TRANSMITTED IS "OF SUCH AN EXTRAORDINARILY SENSITIVE NATURE THAT IT IS REASONABLE TO USE ONLY A MEANS OF COMMUNICATION THAT IS COMPLETELY UNDER THE LAWYER'S CONTROL, THE LAWYER MUST SELECT A MORE SECURE MEANS OF COMMUNICATION THAN UNENCRYPTED INTERNET E-MAIL." SEE ALSO RULE 1.6, CMT. 17 (A LAWYER "MUST TAKE REASONABLE PRECAUTIONS" TO PREVENT INFORMATION COMING INTO THE HANDS OF UNINTENDED RECIPIENTS WHEN TRANSMITTING INFORMATION RELATING TO THE REPRESENTATION, BUT IS NOT REQUIRED TO USE SPECIAL SECURITY MEASURES IF THE MEANS OF COMMUNICATING PROVIDES A REASONABLE EXPECTATION OF PRIVACY).

7. ETHICS ADVISORY OPINIONS IN SEVERAL OTHER STATES HAVE APPROVED THE USE OF ELECTRONIC STORAGE OF CLIENT FILES PROVIDED THAT SUFFICIENT PRECAUTIONS ARE IN PLACE. SEE, E.G., NEW JERSEY OPINION 701 (2006) (LAWYER MAY USE ELECTRONIC FILING SYSTEM WHEREBY ALL DOCUMENTS ARE SCANNED INTO A DIGITIZED FORMAT AND ENTRUSTED TO SOMEONE OUTSIDE THE FIRM PROVIDED THAT THE LAWYER EXERCISES "REASONABLE CARE," WHICH INCLUDES ENTRUSTING DOCUMENTS TO A THIRD PARTY WITH AN ENFORCEABLE OBLIGATION TO PRESERVE CONFIDENTIALITY AND SECURITY, AND EMPLOYING AVAILABLE TECHNOLOGY TO GUARD AGAINST REASONABLY FORESEEABLE ATTEMPTS TO INFILTRATE DATA);

ARIZONA OPINION 05-04 (2005) (ELECTRONIC STORAGE OF CLIENT FILES IS PERMISSIBLE PROVIDED LAWYERS AND LAW FIRMS "TAKE COMPETENT AND REASONABLE STEPS TO ASSURE THAT THE CLIENT'S CONFIDENCES ARE NOT DISCLOSED TO THIRD PARTIES THROUGH THEFT OR INADVERTENCE"); SEE ALSO ARIZONA OPINION 09-04 (2009) (LAWYER MAY PROVIDE CLIENTS WITH AN ONLINE FILE STORAGE AND RETRIEVAL SYSTEM THAT CLIENTS MAY ACCESS, PROVIDED LAWYER TAKES REASONABLE PRECAUTIONS TO PROTECT SECURITY AND CONFIDENTIALITY AND LAWYER PERIODICALLY REVIEWS SECURITY MEASURES AS TECHNOLOGY ADVANCES OVER TIME TO ENSURE THAT THE CONFIDENTIALITY OF CLIENT INFORMATION REMAINS REASONABLY PROTECTED).

8. BECAUSE THE INQUIRING LAWYER WILL USE THE ONLINE DATA STORAGE SYSTEM FOR THE PURPOSE OF PRESERVING CLIENT INFORMATION - A PURPOSE BOTH RELATED TO THE RETENTION AND NECESSARY TO PROVIDING LEGAL SERVICES TO THE CLIENT - USING THE ONLINE SYSTEM IS CONSISTENT WITH CONDUCT THAT THIS COMMITTEE HAS DEEMED ETHICALLY PERMISSIBLE. *SEE* N.Y. STATE 473 (1977) (ABSENT CLIENT'S OBJECTION, LAWYER MAY PROVIDE CONFIDENTIAL INFORMATION TO OUTSIDE SERVICE AGENCY FOR LEGITIMATE PURPOSES RELATING TO THE REPRESENTATION PROVIDED THAT THE LAWYER EXERCISES CARE IN THE SELECTION OF THE AGENCY AND CAUTIONS THE AGENCY TO KEEP THE INFORMATION CONFIDENTIAL); *CF.* NY CPLR 4548 (PRIVILEGED COMMUNICATION DOES NOT LOSE ITS PRIVILEGED CHARACTER SOLELY BECAUSE IT IS COMMUNICATED BY ELECTRONIC MEANS OR BECAUSE "PERSONS NECESSARY FOR THE DELIVERY OR FACILITATION OF SUCH ELECTRONIC COMMUNICATION MAY HAVE ACCESS TO" ITS CONTENTS).

9. WE CONCLUDE THAT A LAWYER MAY USE AN ONLINE "CLOUD" COMPUTER DATA BACKUP SYSTEM TO STORE CLIENT FILES PROVIDED THAT THE LAWYER TAKES REASONABLE CARE TO ENSURE THAT THE SYSTEM IS SECURE AND THAT CLIENT CONFIDENTIALITY WILL BE MAINTAINED. "REASONABLE CARE" TO PROTECT A CLIENT'S CONFIDENTIAL INFORMATION AGAINST UNAUTHORIZED DISCLOSURE MAY INCLUDE CONSIDERATION OF THE FOLLOWING STEPS:

(1) ENSURING THAT THE ONLINE DATA STORAGE PROVIDER HAS AN ENFORCEABLE OBLIGATION TO PRESERVE CONFIDENTIALITY AND SECURITY, AND THAT THE PROVIDER WILL NOTIFY THE LAWYER IF SERVED WITH PROCESS REQUIRING THE PRODUCTION OF CLIENT INFORMATION;

(2) INVESTIGATING THE ONLINE DATA STORAGE PROVIDER'S SECURITY MEASURES, POLICIES, RECOVERABILITY METHODS, AND OTHER PROCEDURES TO DETERMINE IF THEY ARE ADEQUATE UNDER THE CIRCUMSTANCES;

(3) EMPLOYING AVAILABLE TECHNOLOGY TO GUARD AGAINST REASONABLY FORESEEABLE ATTEMPTS TO INFILTRATE THE DATA THAT IS STORED; AND/OR

(4) INVESTIGATING THE STORAGE PROVIDER'S ABILITY TO PURGE AND WIPE ANY COPIES OF THE DATA, AND TO MOVE THE DATA TO A DIFFERENT HOST, IF THE LAWYER BECOMES DISSATISFIED WITH THE STORAGE PROVIDER OR FOR OTHER REASONS CHANGES STORAGE PROVIDERS.

10. TECHNOLOGY AND THE SECURITY OF STORED DATA ARE CHANGING RAPIDLY. EVEN AFTER TAKING SOME OR ALL OF THESE STEPS (OR SIMILAR STEPS), THEREFORE, THE LAWYER SHOULD PERIODICALLY RECONFIRM THAT THE PROVIDER'S SECURITY MEASURES REMAIN EFFECTIVE IN LIGHT OF ADVANCES IN TECHNOLOGY. IF THE LAWYER LEARNS INFORMATION SUGGESTING THAT THE SECURITY MEASURES USED BY THE ONLINE DATA STORAGE PROVIDER ARE INSUFFICIENT TO ADEQUATELY PROTECT THE CONFIDENTIALITY OF CLIENT INFORMATION, OR 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, NOTIFY ANY AFFECTED CLIENTS, AND DISCONTINUE USE OF THE SERVICE UNLESS THE LAWYER RECEIVES ASSURANCES THAT ANY SECURITY ISSUES HAVE BEEN SUFFICIENTLY REMEDIATED. *SEERULE 1.4 (MANDATING COMMUNICATION WITH CLIENTS); SEE ALSON.Y. STATE 820 (2008) (ADDRESSING WEB-BASED EMAIL SERVICES).*

11. NOT ONLY TECHNOLOGY ITSELF BUT ALSO THE LAW RELATING TO TECHNOLOGY AND THE PROTECTION OF CONFIDENTIAL COMMUNICATIONS IS CHANGING RAPIDLY. LAWYERS USING ONLINE STORAGE SYSTEMS (AND ELECTRONIC MEANS OF COMMUNICATION GENERALLY) SHOULD MONITOR THESE LEGAL DEVELOPMENTS, ESPECIALLY REGARDING INSTANCES WHEN USING TECHNOLOGY MAY WAIVE AN OTHERWISE APPLICABLE PRIVILEGE. *SEE, E.G., CITY OF ONTARIO, CALIF. V. QUON*, 130 S. CT. 2619, 177 LED.2D 216 (2010) (HOLDING THAT CITY DID NOT VIOLATE FOURTH AMENDMENT WHEN IT REVIEWED TRANSCRIPTS OF MESSAGES SENT AND RECEIVED BY POLICE OFFICERS ON POLICE DEPARTMENT PAGERS); *SCOTT V. BETH ISRAEL MEDICAL CENTER*, 17 MISC. 3D 934, 847 N.Y.S.2D 436 (N.Y. SUP. 2007) (E-MAILS

BETWEEN HOSPITAL EMPLOYEE AND HIS PERSONAL ATTORNEYS WERE NOT PRIVILEGED BECAUSE EMPLOYER'S POLICY REGARDING COMPUTER USE AND E-MAIL MONITORING STATED THAT EMPLOYEES HAD NO REASONABLE EXPECTATION OF PRIVACY IN E-MAILS SENT OVER THE EMPLOYER'S E-MAIL SERVER). BUT SEE STENGART V. LOVING CARE AGENCY, INC, 201 N.J. 300, 990 A.2D 650 (2010) (DESPITE EMPLOYER'S E-MAIL POLICY STATING THAT COMPANY HAD RIGHT TO REVIEW AND DISCLOSE ALL INFORMATION ON "THE COMPANY'S MEDIA SYSTEMS AND SERVICES" AND THAT E-MAILS WERE "NOT TO BE CONSIDERED PRIVATE OR PERSONAL" TO ANY EMPLOYEES, COMPANY VIOLATED EMPLOYEE'S ATTORNEY-CLIENT PRIVILEGE BY REVIEWING E-MAILS SENT TO EMPLOYEE'S PERSONAL ATTORNEY ON EMPLOYER'S LAPTOP THROUGH EMPLOYEE'S PERSONAL, PASSWORD-PROTECTED E-MAIL ACCOUNT).

12. THIS COMMITTEE'S PRIOR OPINIONS HAVE ADDRESSED THE DISCLOSURE OF CONFIDENTIAL INFORMATION IN METADATA AND THE PERILS OF PRACTICING LAW OVER THE INTERNET. WE HAVE NOTED IN THOSE OPINIONS THAT THE DUTY TO "EXERCISE REASONABLE CARE" TO PREVENT DISCLOSURE OF CONFIDENTIAL INFORMATION "MAY, IN SOME CIRCUMSTANCES, CALL FOR THE LAWYER TO STAY ABREAST OF TECHNOLOGICAL ADVANCES AND THE POTENTIAL RISKS" IN TRANSMITTING INFORMATION ELECTRONICALLY. N.Y. STATE 782 (2004), CITING N.Y. STATE 709 (1998) (WHEN CONDUCTING TRADEMARK PRACTICE OVER THE INTERNET, LAWYER HAD DUTY TO "STAY ABREAST OF THIS EVOLVING TECHNOLOGY TO ASSESS ANY CHANGES IN THE LIKELIHOOD OF INTERCEPTION AS WELL AS THE AVAILABILITY OF IMPROVED TECHNOLOGIES THAT MAY REDUCE SUCH RISKS AT REASONABLE COST"); SEE ALSON.Y. STATE 820 (2008) (SAME IN CONTEXT OF USING E-MAIL SERVICE PROVIDER THAT SCANS E-MAILS TO GENERATE COMPUTER ADVERTISING). THE SAME DUTY TO STAY CURRENT WITH THE TECHNOLOGICAL ADVANCES APPLIES TO A LAWYER'S CONTEMPLATED USE OF AN ONLINE DATA STORAGE SYSTEM.

CONCLUSION

13. A LAWYER MAY USE AN ONLINE DATA STORAGE SYSTEM TO STORE AND BACK UP CLIENT CONFIDENTIAL INFORMATION PROVIDED THAT THE LAWYER TAKES REASONABLE CARE TO ENSURE THAT CONFIDENTIALITY IS MAINTAINED IN A MANNER CONSISTENT WITH THE LAWYER'S OBLIGATIONS UNDER RULE 1.6. A LAWYER USING AN ONLINE STORAGE PROVIDER SHOULD TAKE REASONABLE CARE TO PROTECT CONFIDENTIAL INFORMATION, AND SHOULD EXERCISE REASONABLE CARE TO PREVENT OTHERS WHOSE SERVICES ARE UTILIZED BY THE LAWYER FROM DISCLOSING OR USING CONFIDENTIAL INFORMATION OF A CLIENT. IN ADDITION, THE LAWYER SHOULD STAY ABREAST OF TECHNOLOGICAL ADVANCES TO ENSURE THAT THE STORAGE SYSTEM REMAINS SUFFICIENTLY ADVANCED TO PROTECT THE CLIENT'S INFORMATION,

AND THE LAWYER SHOULD MONITOR THE CHANGING LAW OF PRIVILEGE TO ENSURE THAT STORING INFORMATION IN THE "CLOUD" WILL NOT WAIVE OR JEOPARDIZE ANY PRIVILEGE PROTECTING THE INFORMATION.

(75-09)

One Elk Street, Albany , NY 12207
Phone: 518-463-3200 Secure Fax: 518.463.5993

© 2016 New York State Bar Association



NEW YORK STATE BAR ASSOCIATION
Serving the legal profession and the community since 1876

ETHICS OPINION 1019

New York State Bar Association
Committee on Professional Ethics

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

QUESTION

1. May a law firm provide its lawyers with remote access to its electronic files, so that they may work from home?

OPINION

2. Our committee has often been asked about the application of New York's ethical rules -- now the Rules of Professional Conduct -- to the use of modern technology. While some of our technology opinions involve the application of the advertising rules to advertising using electronic means, many involve other ethical issues. See, e.g.:

N.Y. State 680 (1996). Retaining records by electronic imaging during the period required by DR 9-102 (D) [now Rule 1.15(d)].

N.Y. State 709 (1998). Operating a trademark law practice over the internet and using e-mail.

N.Y. State 782 (2004). Use of electronic documents that may contain "metadata".

N.Y. State 820 (2008). Use of an e-mail service provider that conducts computer scans of emails to generate computer advertising.

N.Y. State 833 (2009). Whether a lawyer must respond to unsolicited emails requesting representation.

N.Y. State 842 (2010). Use of a "cloud" data storage system to store and back up client confidential information.

N.Y. State 940 (2012). Storage of confidential information on off-site backup tapes.

N.Y. State 950 (2012). Storage of emails in electronic rather than paper form.

3. Much of our advice in these opinions turns on whether the use of technology would violate the lawyer's duty to preserve the confidential information of the client. Rule 1.6(a) sets forth a simple prohibition against disclosure of such information, i.e. "A lawyer shall not knowingly reveal confidential information, as defined in this Rule . . . unless . . . the client gives informed consent, as defined in Rule 1.0(j)." In addition, Rule 1.6(c) provides that a lawyer must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except as provided in Rule 1.6(b).

4. Comment 17 to Rule 1.6 provides some additional guidance that reflects the advent of the information age:

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

5. As is clear from Comment 17, the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology.

6. In some of our early opinions, despite language indicating that the inquiring lawyer must make the reasonableness determination, this Committee had reached general conclusions. In N.Y. State 709, we concluded that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication, such as telephone or fax machine, and that a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. We also noted, however, that "when the confidential information is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted internet e-mail." Moreover, we said the lawyer was obligated to stay abreast of evolving technology to assess changes in the likelihood of interception, as well as the availability of improved technologies that might reduce the risks at a reasonable cost.

7. In N.Y. State 820, we approved the use of an internet service provider that scanned e-mails to assist in providing user-targeted advertising, in part based on the published privacy policies of the provider.

8. Our more recent opinions, however, put the determination of reasonableness squarely on the inquiring lawyer. See, e.g. N.Y. State 842, 940, 950. For example, in N.Y. State 842, involving the use of "cloud" data storage, we were told that the storage system was password protected and that data

stored in the system was encrypted. We concluded that the lawyer could use such a system, but only if the lawyer took reasonable care to ensure that the system was secure and that client confidentiality would be maintained. We said that "reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

- (1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
- (2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
- (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
- (4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

Moreover, in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated.

9. 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. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent); Joe Dysart, "Moving Targets: New Hacker Technology Threatens Lawyers' Mobile Devices," ABA Journal 25 (September 2012); Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal 32 (June 2013); Sharon D. Nelson, John W. Simek & David G. Ries, *Locked Down: Information Security for Lawyers* (ABA Section of Law Practice Management, 2012).

10. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential

information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information. However, assuming that the law firm determines that its precautions are reasonable, we believe it may provide such remote access. When the law firm is able to make a determination of reasonableness, we do not believe that client consent is necessary.

11. Where a law firm cannot conclude that its precautions would provide reasonable protection to client confidential information, Rule 1.6(a) allows the law firm to request the client's informed consent. See also Comment 17 to Rule 1.6, which provides that a client may give informed consent (as in an engagement letter or similar document) to the use of means that would otherwise be prohibited by the rule. In N.Y. State 842, however, we stated that the obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must take reasonable care to affirmatively protect a client's confidential information. Consequently, we believe that before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision.

CONCLUSION

12. A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firm discloses the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0 (j).

7-14



NEW YORK STATE BAR ASSOCIATION
Serving the legal profession and the community since 1876

ETHICS OPINION 1020

New York State Bar Association
Committee on Professional Ethics

Opinion 1020 (9/12/2014)

Topic: Confidentiality; use of cloud storage for purposes of a transaction

Digest: Whether a lawyer to a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

Rules: 1.1, 1.6

FACTS

1. The inquirer is engaged in a real estate practice and is looking into the viability of using an electronic project management tool to help with closings. The technology would allow sellers' attorneys, buyers' attorneys, real estate brokers and mortgage brokers to post and view documents, such as drafts, signed contracts and building financials, all in one central place.

QUESTION

2. May a lawyer representing a party to a transaction use a cloud-based technology so as to post documents and share them with others involved in the transaction?

OPINION

3. The materials that the inquirer seeks to post, such as drafts, contracts and building financials, may well include confidential information of the inquirer's clients, and for purposes of this opinion we assume that they do.¹ Thus the answer to this inquiry hinges on whether use of the contemplated technology would violate the inquirer's ethical duty to preserve a client's confidential information.

4. Rule 1.6(a) contains a straightforward prohibition against the knowing disclosure of confidential information, subject to certain exceptions including a client's informed consent, and Rule 1.6(c) contains the accompanying general requirement that a lawyer "exercise reasonable care to prevent ... [persons] whose services are utilized by the lawyer from disclosing or using confidential information of a client."

5. Comment [17] to Rule 1.6 addresses issues raised by a lawyer's use of technology:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

6. In the recent past, our Committee has repeatedly been asked to provide guidance on the interplay of technology and confidentiality. N.Y. State 1019 (2014) catalogues the Committee's opinions on technology. In that opinion, we considered whether a law firm could provide its lawyers with remote access to its electronic files. We concluded that a law firm could use remote access "as long as it takes reasonable steps to ensure that confidential information is maintained." *Id.* ¶12

7. Similarly, in N.Y. State 842 (2010), which considered the use of cloud data storage, we concluded that a lawyer could use this technology to store client records provided that the lawyer takes reasonable care to protect the client's confidential information. We also reached a similar conclusion in N.Y. State 939 (2012) as to the issue of lawyers from different firms sharing a computer system.

8. The concerns presented by the current inquiry were also present in N.Y. State 1019, N.Y. State 939 and N.Y. State 842, and those opinions govern the outcome here. That is, the inquirer may use the proposed technology provided that the lawyer takes reasonable steps to ensure that confidential information is not breached.² The inquirer must, for example, try to ensure that only authorized parties have access to the system on which the information is shared. Because of the fact-specific and evolving nature of technology, we do not purport to specify in detail the steps that will constitute reasonable care in any given set of circumstances. See N.Y. State 1019, ¶10. We note, however, that use of electronically stored information may not only require reasonable care to protect that information under Rule 1.6, but may also, under Rule 1.1, require the competence to determine and follow a set of steps that will constitute such reasonable care.³

9. Finally, we note that Rule 1.6 provides an exception to confidentiality rules based on a client's informed consent. Thus, as quoted in paragraph 5 above, a client may agree to the use of a technology that would otherwise be prohibited by the Rule. But as we have previously pointed out, "before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is 'informed' within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision." N.Y. State 1019 ¶11.

CONCLUSION

10. Whether a lawyer for a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

(17-14)

¹Rule 1.6(a) defines "confidential information" generally to include "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

²This result is consistent with results in other jurisdictions that have considered lawyers' use of off-site, third-party cloud services for storing and sharing documents. *See, e.g.*, ABA 95-398; Arizona Opinion 05-04; California Opinion 2010-179; Connecticut Inf. Opinion 2013-07; Florida Opinion 12-3 (2013); Illinois Opinion 10-01 (2009); Iowa Opinion 11-01; Maine Opinion 207 (2013); Massachusetts Opinion 12-03; Massachusetts Opinion 05-04; Missouri Inf. Opinion 2006-0092; Nebraska Opinion 06-05; New Hampshire Opinion 2012-13/4 (2013); New Jersey Opinion 701 (2006); North Carolina Opinion 2011-6 (2012); North Dakota Opinion 99-03 (1999); Ohio Opinion 2013-03; Oregon Opinion 2011-188; Pennsylvania Opinion 2011-200; Pennsylvania Opinion 2010-060; Vermont Opinion 2010-6 (2012); Washington Inf. Opinion 2215 (2012).

³It has been said for example that the duty of competence may require litigators, depending on circumstances, to possess a basic or even a more refined understanding of electronically stored information. *See, e.g.*, Zachary Wang, "Ethics and Electronic Discovery: New Medium, Same Problems," 75 Defense Counsel Journal 328, at 7 (October 2008) ("disclosure of privileged information as a result of a lack of knowledge of a client's IT system would subject an attorney to discipline under Rules 1.1 and 1.6"). The California State Bar Standing Committee on Professional Responsibility and Conduct has tentatively approved an interim opinion interpreting California ethical rules as follows:

Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. ... An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.

COPRAC Proposed Formal Opinion 11-0004 (2014).

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

Formal Opinion 2015-3: LAWYERS WHO FALL VICTIM TO INTERNET SCAMS

TOPIC: Internet-based scams targeting law firms

DIGEST: An attorney who discovers that he is the target of an Internet-based trust account scam does not have a duty of confidentiality towards the individual attempting to defraud him, and is free to report the individual to law enforcement authorities, because that person does not qualify as a prospective or actual client of the attorney. However, before concluding that an individual is attempting to defraud the attorney and is not owed the duties normally owed to a prospective or actual client, the attorney must exercise reasonable diligence to investigate whether the person is engaged in fraud. In addition, because Internet-based trust account scams may harm other firm clients, a lawyer who receives a request for representation via the Internet has a duty to conduct a reasonable investigation to ascertain whether the person is a legitimate prospective client before accepting the representation. A lawyer who discovers he has been defrauded in a manner that results in harm to other clients of the law firm, such as the loss of client funds due to an escrow account scam, must promptly notify the harmed clients.

RULES: 1.1, 1.4, 1.6, 1.15, and 1.18

QUESTION: What are the ethical duties of a lawyer upon suspecting or discovering that he is the target of an Internet-based trust account scam?

OPINION:

I. INTRODUCTION

Internet-based scams targeting lawyers are not new and appear to be on the rise.¹ Since 2009, email scams have swindled lawyers out of an estimated \$70 million.² These scams are often highly sophisticated, involving parties that appear to be representing legitimate international corporations and using high-quality counterfeit checks that can take a bank weeks

¹ See, e.g., Jennifer Smith, *In Email, Scammers Take Aim At Lawyers*, Wall St. J., Aug. 5, 2012, <http://www.wsj.com/articles/SB10000872396390443517104577571453933076304>; James McCauley, *Increasingly Sophisticated Internet Scams Continue to Target Lawyers*, Va. State Bar, Dec. 2, 2013, <http://www.vsb.org/site/news/item/increasingly-sophisticated-internet-scams-continue-to-target-lawyers>; Todd C. Scott, *Scammed! Sophisticated Check Fraud Scheme Targets Lawyers*, Am. Bar Ass'n Law Trends & News, Fall 2010, Vol. 7, No.1., available at http://www.americanbar.org/content/newsletter/publications/law_trends_news_practice_area_e_newsletter_home/10_fall_pm_feat1.html.

² Smith, *supra* note 1.

to discover. One experienced ring obtained \$29 million over a two-year period from seventy lawyers in the United States and Canada.³ Once an attorney falls victim to a scam, his problems have just begun. Banks have sued attorneys for lost funds caused by counterfeit checks, and some malpractice insurers have refused to indemnify affected lawyers. *See e.g., Lombardi, Walsh, Wakeman, Harrison, Amodeo & Davenport, P.C. v. American Guarantee and Liab. Ins. Co.*, 924 N.Y.S.2d 201 (3d Dep't 2011) (coverage litigation between insurer and attorney, arising from settlement of bank's lawsuit against attorney as a result of an overdraft caused by a counterfeit check); *O'Brien & Wolf, L.L.P. v. Liberty Ins. Underwriters Inc.*, No. 11-cv-3748, 2012 WL 3156802 (D. Minn. Aug. 3, 2012) (holding that insurance company was required to cover losses from attorney trust account due to counterfeit check scheme); *Attorneys Liab. Protection Soc., Inc. v. Whittington Law Assocs., PLLC*, 961 F.Supp.2d 367 (D. N.H. 2013) (denying insurance coverage for losses due to "Nigerian check scam").⁴ On top of that, a law firm that suspects or knows that it is a victim of an Internet scam faces serious questions about its ethical obligations. This opinion addresses some of those ethical issues and offers guidance to attorneys who believe they are (or have been) the target of an Internet scam.

II. A TYPICAL SCAM⁵

A common example of the internet-based scam begins with an email from an individual requesting assistance with an urgent transactional or litigation matter (the "email sender"). This email sender is generally located abroad, whereas the counterparty or adversary is usually located in the attorney's jurisdiction. The email sender often proposes a contingency fee arrangement whereby the attorney would receive a percentage of the transaction total or litigation settlement. If the attorney sends a draft engagement letter, the email sender swiftly executes it. Soon thereafter, the email sender notifies the attorney that transaction has been consummated or the litigation has settled. As a result, the attorney performs little or no work before the engagement ends.

³ McCauley, *supra* note 1.

⁴ A determining factor in lawyer-insurer litigation surrounding scams is often whether or not the activity was related to the firm's "professional" services. *See, e.g., Bradford & Bradford, P.A. v. Attorneys Liab. Prot. Soc'y, Inc.*, No. 0:09-CV-02981-CMC 2010 WL 4225907 (D.S.C. Oct. 20, 2010) (no duty to defend law firm against lawsuit by bank to recover funds lost due to trust account fraud). In New York, however, at least one appellate court has held that handling a client's funds is part of the legal services provided, even when the client is an imposter. *Lombardi*, 924 N.Y.S.2d 201 (insurance company required to defend law firm against lawsuit by bank for lost funds). We highlight these cases merely to alert attorneys to the insurance coverage issues; whether or not losses caused by Internet-based scams are covered by legal malpractice insurance is outside the Committee's jurisdiction, which is limited to interpreting the New York Rules of Professional Conduct.

⁵ This description of the typical scam and the "red flags" identified in Sections II and III are derived from case law, articles, and ethics opinions cited throughout this opinion.

The attorney receives the closing or settlement check quickly. The attorney then deposits the check in the law firm's trust account and, once the check has "cleared," the attorney transfers his contingent fee into his operating account and wires the remainder of the funds to a foreign bank account designated by the email sender. Unfortunately, the attorney might not realize that a bank can "clear" a check and make the funds available before the bank actually *collects* the funds. The bank may take weeks or even months to discover that the check is fraudulent. When that happens, the bank will notify the attorney that the check was fraudulent.

If the trust account contains the funds of other clients, then those clients may be harmed because the bank may use those funds to cover all or part of the wire transfer. If the trust account contains no other client funds (or if the client funds are insufficient to cover the full amount of the wire transfer), then the bank will notify the attorney that his trust account is overdrawn, and will look to the attorney or the law firm to make up the deficiency.

III. RED FLAGS WHICH MAY ALERT AN ATTORNEY TO AN INTERNET SCAM

Before we discuss an attorney's ethical options and obligations upon receiving a scam communication, we will identify some of the elements that may alert an attorney to the scam. A lawyer's suspicion should be aroused by any one or more of these common "red flags" indicating a scam:

- The email sender is based abroad.
- The email sender does not provide a referral source. (If the email sender is asked how he found the firm, he may respond that it was through an online search. If prospective clients rarely approach the recipient attorney based on an Internet search, this should be an immediate red flag.)
- The initial email does not identify the law firm or recipient attorney by name, instead using a salutation such as "Dear barrister/solicitor/counselor."
- The email uses awkward phrasing or poor grammar, suggesting that it was written by someone with poor English or was converted into English via a translation tool.
- The email is sent to "undisclosed recipients," suggesting that it is directed to multiple recipients. (Alternatively, the attorney recipient may be blind copied on the email.)
- The email requests assistance on a legal matter in an area of law the recipient attorney does not practice.
- The email is vague in other respects, such as stating that the sender has a matter in the attorney's "jurisdiction," rather than specifying the jurisdiction itself.
- The email sender suggests that for this particular matter the attorney accept a contingency fee arrangement, even though that might not be customary for the attorney's practice.
- The email sender is quick to sign a retainer agreement, without negotiating over the attorney's fee (since the fee is illusory anyway).
- The email sender assures the attorney that the matter will resolve quickly.
- The counterparty, if there is one, will also likely respond quickly, settling the dispute or closing the deal with little or no negotiation.

- The email sender insists that his funds must be wired to a foreign bank account as soon as the check has cleared. (The sender often claims that there is an emergency requiring the immediate release of the funds.)
- The email sender or counterparty sends a supposed closing payment or settlement check within a few days. The check is typically a certified check or a cashier's check, often from a bank located outside of the attorney's jurisdiction.

IV. DUTIES OF A LAWYER WHO SUSPECTS OR LEARNS THAT HE IS THE TARGET OF AN INTERNET SCAM

When an attorney receives an email from what appears to be a prospective client, it may not be immediately obvious whether it is a legitimate inquiry or an Internet scam. The email sender may provide contracts or other legal documents that look completely genuine; the companies involved in the transaction or litigation may have realistic websites; and the closing or settlement check that the attorney receives may be so authentic looking that even a bank has difficulty detecting that it is fraudulent.

Consequently, if an email or the course of dealing with the client contains one or more of the red flags described above, the safest course may be to delete it. As the California State Bar Association Committee on Professional Responsibility and Conduct ("COPRAC") has noted: "The best approach is to ignore such solicitations altogether." COPRAC Ethics Alert: *Internet Scams Targeting Lawyers* (Jan. 2011). An attorney has no ethical obligation to respond to an unsolicited email inquiry from a prospective client. See NYSBA Ethics Op. 833 (2009) ("An attorney is not ethically required to respond to unsolicited letters from incarcerated individuals requesting legal representation."). If the attorney responds to the email, however, he should be mindful of certain ethical obligations that arise once he engages in those communications.

A. Ethical Duties Owed to the Email Sender

Even before an attorney-client relationship has formed, an attorney owes certain duties to prospective clients, including the duty to preserve confidential information. See Rule 1.18(b). Those duties do not apply, however, to someone who is merely posing as a "prospective client" but whose purpose is to defraud the attorney. The Committee on Professional Ethics of the New York State Bar Association ("NYSBA") has noted:

[A] person who communicates with a lawyer seemingly for the purpose of forming a relationship to obtain legal services is presumptively a "prospective client" entitled to protections of confidentiality under the Rules. However, if the purported prospective client is actually seeking to defraud the lawyer rather than to obtain legal services, then the person is neither an actual nor a prospective client and is not entitled to those confidentiality protections.

NYSBA Ethics Op. 923 (May 18, 2012) (emphasis added). In light of these principles, an attorney must exercise diligence in investigating prospective clients before concluding that they

are not genuine and thus not owed any ethical obligations. “The presumption of confidentiality gives way only if and when the lawyer reasonably concludes that the purported client was not actually seeking legal services.” *Id.*

While an attorney is investigating the validity of a potential new matter, he is still bound by his duties to a legitimate prospective client. In particular, Rule 1.18(b) prohibits the disclosure of any information learned in the consultation with the prospective client. If the attorney has not yet determined that the prospective client is trying to defraud the attorney, then the attorney is prohibited from disclosing confidential information about the client, including to banking and law enforcement authorities. If the attorney concludes after investigating the matter that the email sender is attempting to defraud him, then the attorney “may report the scheme to affected banks or law enforcement authorities, and may supply information and documents to those investigating the scheme, without violating any duty of confidentiality that would be owed to persons genuinely seeking legal services.” *Id.*

B. Ethical Duties Owed to Other Clients of the Firm

When an attorney falls victim to the type of Internet scam described above, it could place other clients of the firm at risk. For example, if an attorney’s trust account holds funds from multiple clients, then any funds that are transferred from the trust account to the email sender most likely belong to other clients of the firm. This would place the firm in violation of Rule 1.15(a), which imposes a fiduciary duty upon the attorney to preserve client funds. The loss of those client funds triggers other ethical obligations, including a duty to immediately notify all affected clients. *See* Rule 1.4(a)(1)(iii) (lawyer must “promptly inform the client of . . . material developments in the matter”).

In addition to suffering the reputational damage and financial losses that may come with falling victim to a scam, a lawyer may have violated the duty of competence. Rule 1.1 requires a lawyer to provide competent legal representation to a client and not to “intentionally . . . prejudice or damage the client during the course of the representation except as permitted or required by these Rules.” Rule 1.1(a), 1.1(c)(2). In our view, the duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding common Internet-based scams, particularly where those scams can harm other existing clients. Since depositing a counterfeit check into a firm’s trust account can negatively impact an attorney’s other current clients whose funds are in the same account, an attorney who fails to exercise reasonable diligence to identify and avoid an Internet scam may violate Rule 1.1. *See Iowa Sup. Ct. Att’y Disciplinary Bd. v. Wright*, 840 N.W.2d 295 (Iowa 2013) (attorney violated duty of competence by failing to conduct a cursory Internet search, which would have revealed the existence of a commonplace internet scam that resulted in financial loss to attorney’s other clients).

Thus, an attorney who receives an email solicitation from an unknown individual should conduct a reasonable investigation to ascertain that the email sender is a legitimate prospective client. The due diligence may include verifying the accuracy of the information provided by the email sender, such as names, addresses, telephone numbers, website addresses, and referral sources. The attorney should resist the temptation to depart from his customary intake procedures, such as performing conflict checks, verifying the prospective client’s business and

financial status, executing a retainer agreement, and obtaining an advance retainer. The attorney should also take reasonable steps to ensure that all funds deposited into the trust account are held until the bank confirms that the funds have been honored or collected, not merely that a check has "cleared." As noted above, pressure from the email sender to wire the funds immediately on the basis of an emergency or urgent need is a red flag that should be scrutinized more closely.

V. CONCLUSION

An attorney who discovers that he is the target of an Internet-based trust account scam does not have a duty of confidentiality towards the individual attempting to defraud him, and is free to report the individual to law enforcement authorities, because that person does not qualify as a prospective or actual client of the attorney. However, before concluding that an individual is attempting to defraud the attorney and is not owed the duties normally owed to a prospective or actual client, the attorney must exercise reasonable diligence to investigate whether the person is engaged in fraud. In addition, because Internet-based trust account scams may harm other firm clients, a lawyer who receives a request for representation via the Internet has a duty to conduct a reasonable investigation to ascertain whether the person is a legitimate prospective client before accepting the representation. A lawyer who discovers he has been defrauded in a manner that results in harm to other clients of the law firm, such as the loss of client funds due to an escrow account scam, must promptly notify the harmed clients.

MOSES & SINGER LLP

Ethical Obligations in Cyber Security:
The Risks You Must Know, The Responsibilities You Cannot Avoid

Presented By: Devika Kewalramani
July 14, 2018

© 2018 Moses & Singer LLP 3966613

MOSES & SINGER LLP

2 Overview


- Ethical duties relating to cyber security
- Guidance by bar associations
- Emerging law firm cyber security breach cases

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

3 Ethical Duties Relating to Cyber Security

- Duty of competence (Rule 1.1); Comment [8]
- Duty to communicate (Rule 1.4)
- Duty of confidentiality (Rule 1.6); Comment [17]
- Duty to make reasonable efforts to ensure ethical compliance (Rule 5.1)
- Duty to adequately supervise non-lawyers (Rule 5.3); Comments [2] & [3]



Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

4 Ethical Duties Relating to Cyber Security


- Competence: Keep abreast of benefits/risks associated with use of technology in legal services
- Communication: Reasonably consult with client about means to accomplish client's objectives
- Confidentiality: Reasonable care to prevent unauthorized access or inadvertent disclosure
- Reasonable efforts to ensure ethical compliance
- Ensure non-lawyer conduct is compatible with professional obligations of lawyer

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

5 Guidance By Bar Associations

- N.Y. State Bar Opinion 842 (2010)
- N.Y. State Bar Opinion 1020 (2014)
- N.Y. State Bar Opinion 1019 (2014)
- CA State Bar Opinion 2010-179 (2010)
- ABA Opinion 477 (2017)
- N.Y. City Bar Opinion 2015-3 (2015)



Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

6 Guidance By Bar Associations

Using outside online storage provider to store confidential client data (State Bar Opinion 842)

- "Reasonable care" standard to protect client against unauthorized disclosure
- Duty to keep up with advances in technology
- Monitor changing law of privilege to avoid loss of privilege
- Steps to take if there is a data breach

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

7 Guidance By Bar Associations

Posting/sharing documents using cloud data storage tool in a transaction (State Bar Opinion 1020)

- Take reasonable measures to ensure client confidential data is not breached
- Duty of confidentiality ties in with duty of competence

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

8 Guidance By Bar Associations

Remote access to firm's electronic files (State Bar Opinion 1019)

- Does particular technology provide reasonable protection to client data or has client consented after being informed of cyber risks?
- Recognizes cyber security threats to law firms but does not specify what reasonable precautions to take to prevent unintended disclosure

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

9 Guidance By Bar Associations

Using laptop in local coffee shop for legal research via public wireless Internet (CA Opinion 2010-179)

- Steps to evaluate if duties of confidentiality and competence violated when using particular technology:
 - Level of security attendant to use of that technology
 - Legal ramifications to third party interceptor
 - Degree of sensitivity of data
 - Possible impact on client of inadvertent disclosure
 - Urgency of situation
 - Client's instructions and circumstances

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

10

Guidance By Bar Associations

Securing Communication of Protected Client Information (ABA Opinion 477)

- Updated Guidance in light of increasing cybersecurity threats and technology advances
- Case-by-case analysis of electronic communications about client matters
 - Is data sensitive?
 - How is data accessed and managed?
 - What security measures provide reasonable protection?
 - Discuss level of security with client
 - Label as "privileged and confidential"
 - Security training for legal/nonlegal personnel
 - Conduct due diligence on third-party vendors

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

MOSES & SINGER LLP

11

Guidance By Bar Associations

Internet scams targeting law firms (City Bar Opinion 2015-3)

- Exercise reasonable diligence to investigate
- Owe duty of confidentiality?
- Reporting to law enforcement
- Notice to clients who may be harmed

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

12

Emerging Law Firm Cyber Security Breach Cases

- *Millard v. Doran*, filed in N.Y. State Supreme Court, April 2016
- *Jason Shore and Coinabul, LLC v. Johnson & Bell, Ltd.*, filed in Northern District, Illinois, April 2016

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613

13

Questions?

Contact: Devika Kewalramani, Esq.
Partner
Moses & Singer LLP
405 Lexington Avenue
New York, NY 10174-1299
Telephone: 212-554-7832
E-mail: dkewalramani@mosessinger.com

Disclaimer: This presentation does not constitute legal advice or an opinion of Moses & Singer LLP or any member of the firm. It does not create or invite an attorney-client relationship and may be rendered incorrect by future developments. It is recommended that it not be relied upon in connection with any dispute or other matter but that professional advice be sought.

Attorney Advertising: Under the laws, rules or regulations of certain jurisdictions, this presentation may be construed as an advertisement or solicitation.

Copyright © 2018 Moses & Singer LLP. All rights reserved.

Ethical Obligations in Cyber Security: The Risks You Must Know, The Responsibilities You Cannot Avoid 3966613
