Published on *The National Law Review* (http://www.natlawreview.com)

5 Cybersecurity Risks and 3 Obligations for Law Firms

Article By:
Dr. Nick Oberheiden

Law firms have recently become prime targets for cybercriminals seeking to steal, expose, sell, or otherwise extort confidential information. Both the digitalization of law firms' sensitive documents and the increase in means available to perpetrate an online crime exacerbate these risks. Law firms encounter various cybersecurity risks from "insiders"—personnel within the company—and external persons.

As a response, many law firms have adopted cybersecurity obligations to protect its clients' data and the firm's integrity and reputation.

Main Cybersecurity Risks Facing Law Firms

Law firms naturally handle sensitive client data and confidential company information. The lack of strong internal controls and compliance programs leaves law firms open to cyber-attacks. These attacks can be committed by insiders within the firm as well as external actors. Some examples of cybersecurity risks for law firms include the following:

- **Data breaches:** This risk involves the theft of personal or sensitive data from law firms and can be perpetrated for a variety of reasons including financial gain or retaliatory purposes. Cyber criminals will typically execute these attacks by accessing the law firm's computer from a remote location, collecting the personal or sensitive data, and distributing it to third parties.

- **Ransomware:** Ransomware involves encrypting the law firm's important files and demanding a fee—or ransom—in order for the cyber criminal to restore the file for the law firm's use.

- **Phishing:** This scam involves sending a scam message to an individual(s) in the hopes of getting them to send back confidential information. This risk is especially prevalent in law firms due to the high volume of emails sent from external persons. If severe, the attorney's entire email account could be hacked, thus revealing mounds of sensitive client details.

- **Website attacks:** Attorneys visit multiple legitimate websites in a day as a part of their daily responsibilities. Criminals and hackers exploit this by infecting the computers of individuals who visit less secured websites.

- **Miscellaneous cyber threats:** Additional threats to law firms' security include (1) malpractice lawsuits that follow a breach and (2) cyber-crimes committed by insiders. A client can file a malpractice lawsuit where they believe their attorney has failed to maintain adequate safeguards over their sensitive information. Further, insider threats can originate from former disgruntled employees or current personnel members and are often very challenging to detect because these individuals often have access to the computers storing the data.

FLORIDA BAR ETHICS OPINION
OPINION 21-1
June 10, 2021

Advisory ethics opinions are not binding.

A lawyer may not disclose information concerning a client's representation without the client's informed consent when responding to negative online reviews posted by individuals who are not current clients or former clients. If accurate, the lawyer may state that the person who made the post is not a current client or former client. The lawyer may generally note that the comments in the review are inaccurate but that the lawyer's response is constrained by the lawyer's ethical obligations.

RPC: 4-1.6; 4-1.6(c)
Opinions: 20-1; ABA Formal Opinion 496

The Professional Ethics Committee has been asked by the Board of Governors of The Florida Bar to give an opinion on Florida Bar members responding to negative online reviews posted by individuals that are not clients or former client.

Negative online reviews are becoming more common. Florida Ethics Opinion 20-1 discusses a lawyer's response to a client or former client's negative online review.

Besides clients or former client, often a third party who is close to the client or former client will post a negative review about the lawyer. Occasionally, someone who lacks a connection even to the lawyer will post a negative review.

Rule 4-1.6 is the rule regarding confidentiality of information. Rule 4-1.6(c) explains when a lawyer may reveal confidential information and states:

> **(c) When Lawyer May Reveal Information.** A lawyer may reveal confidential information to the extent the lawyer reasonably believes necessary:
>
> (1) to serve the client's interest unless it is information the client specifically requires not to be disclosed;
>
> (2) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and client;
>
> (3) to establish a defense to a criminal charge or civil claim against the lawyer based on conduct in which the client was involved;
>
> (4) to respond to allegations in any proceeding concerning the lawyer's representation of the client;
>
> (5) to comply with the Rules Regulating The Florida Bar; or
>
> (6) to detect and resolve conflicts of interest between lawyers in different firms arising from the lawyer's change of employment or from changes in the

> composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.

The comment to the rule explains:

> A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation…The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose confidential information except as authorized or required by the Rules Regulating The Florida Bar or by law.

If a lawyer wants to respond to a negative online post by someone who is not a client or former client, the lawyer must still determine whether the response reveals confidential information about a client. If true, a lawyer may respond by stating that the person posting is not a client or former client. A lawyer may also state: "As a lawyer, I am constrained by the Rules Regulating The Florida Bar in responding, but I will simply state that it is my belief that the comments are not accurate." A lawyer owes no ethical duties to a person who is not a client or former client posting a negative online review. However, ABA Formal Opinion 496 warns that "a lawyer must use caution in responding to posts from nonclients." It further states:

> If the negative commentary is by a former opposing party or opposing counsel, or a former client's friend or family member, and relates to an actual representation, the lawyer may not disclose any information relating to the client or former client's representation without the client or former client's informed consent. Even a general disclaimer that the events are not accurately portrayed may reveal that the lawyer was involved in the events mentioned, which could disclose confidential client information. The lawyer is free to seek informed consent of the client or former client to respond, particularly where responding might be in the client or former client's best interests. In doing so, it would be prudent to discuss the proposed content of the response with the client or former client.

In conclusion, when responding to a negative online review by someone who is not a client or former client, the lawyer must still consider Rule 4-1.6 and determine whether the response would reveal confidential information regarding a client or former client's matter. A lawyer may respond in a way that does not reveal confidential information about a client or former client. If true, a lawyer may respond that the poster is not a client or a former client.

FLORIDA BAR ETHICS OPINION
OPINION 20-01
October 9, 2020

Advisory ethics opinions are not binding.

A lawyer may not disclose information relating to a client's representation in response to a negative online review, but may respond with a general statement that the lawyer is not permitted to respond as the lawyer would wish, but that the online review is neither fair nor accurate.

RPC: Preamble, 4-1.6(c)
Opinions: Los Angeles County 525; Nassau County 2016-01; New York State 1032; Pennsylvania 2014-200; Texas 622; West Virginia 2015-02
Cases: *People v. Isaac,* 470 P.3d 837 (Colo. O.P.D.J. 2016); *People v. Underhill,* 2015 WL 4944102 (Colo. O.P.D.J. Aug. 12, 2015); *In re Skinner,* 740 S.E.2d 171 (Ga. 2013)

A member of The Florida Bar has requested an advisory ethics opinion. The operative facts as presented in the inquiring attorney's letter are as follows:

The inquirer received a negative online review and would like to respond to the former client's negative review that the inquirer "took her money and ran" by using the language suggested in Texas Ethics Opinion 662 and adding an objectively verifiable truthful statement that the Court entered an order authorizing the inquirer to withdraw as counsel for the former client. The inquirer believes this added language is proportional and restrained, consistent with the Texas Ethics Opinion, directly addressed the allegations of the former client, and should be permissible under the Rules Regulating the Florida Bar and the First Amendment.

Rule 4-1.6(c) explains when a lawyer may reveal confidential information and states:

> **(c) When Lawyer May Reveal Information.** A lawyer may reveal confidential information to the extent the lawyer reasonably believes necessary:
>
> (1) to serve the client's interest unless it is information the client specifically requires not to be disclosed;
>
> (2) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and client;
>
> (3) to establish a defense to a criminal charge or civil claim against the lawyer based on conduct in which the client was involved;
>
> (4) to respond to allegations in any proceeding concerning the lawyer's representation of the client;
>
> (5) to comply with the Rules Regulating The Florida Bar; or

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

The comment to the rule explains:

A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation…The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose confidential information except as authorized or required by the Rules Regulating The Florida Bar or by law.

In addition, the last paragraph of the comment specifically addresses the lawyer's duty of confidentiality to former clients and explains that the duty of confidentiality continues after the client-lawyer relationship has terminated.

A number of jurisdictions have looked at the issue of responding to negative online reviews. A majority conclude that a lawyer may not disclose confidential information in responding to online reviews. See Los Angeles County Ethics Opinion 525 (an attorney can publicly respond to a former client's disparaging comments only if the attorney's response does not disclose confidential information, the attorney does not respond in a manner that will injure the former client in a matter involving the former representation, and the attorney's response is proportionate and restrained); Nassau County Ethics Opinion 2016-01 (a lawyer may not disclose a former client's confidential information solely to respond to criticism of the lawyer posted on the Internet or a website by a relative of the former client or by the former client himself); New York State Ethics Opinion 1032 (a lawyer may not disclose confidential information just to respond to online criticism by the client on a rating site; the "self-defense" exception to confidentiality does not apply to informal criticism where there is no actual or threatened proceeding against the lawyer); Pennsylvania Ethics Opinion 2014-200 (a lawyer may not give detailed response to online criticism of the lawyer by a client, may just ignore the online criticism; the self-defense exception is not triggered by a negative online review); West Virginia Legal Ethics Opinion 2015-02 (a lawyer may respond to positive or negative online reviews, but may not disclose confidential client information while doing so); *People v. Underhill,* 2015 WL 4944102 (Colo. O.P.D.J. Aug. 12, 2015) (a lawyer was suspended 18 months for responding to clients' online criticism by posting confidential and sensitive information about the clients); *People v. Isaac,* 470 P.3d 837 (Colo. O.P.D.J. 2016)(a lawyer was given a six-month suspension with requirement to apply for reinstatement for responding to online reviews of former clients when the lawyer had revealed confidential information including the criminal charges made against clients, that client wrote a check that had bounced, and that client committed other unrelated felonies); *In re Skinner,* 740 S.E.2d 171 (Ga. 2013)(the Supreme Court of Georgia rejected a petition for voluntary discipline seeking a public reprimand for lawyer's violation of the confidentiality rule by disclosing confidential client information on the Internet in response to client's negative reviews of lawyer, citing lack of information about the violation in the record).

In the instant inquiry, the inquirer does not meet an exception to confidentiality under 4-1.6(c). Because confidentiality covers all information regarding the representation, whatever the source, and because this duty applies to former as well as current clients, the inquirer must not disclose confidential information without the client's informed consent.

The preamble to Chapter 4 of the Rules Regulating The Florida Bar defines informed consent as "the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct."

Therefore, if the inquirer chooses to respond to the negative online review and the inquirer does not obtain the former client's informed consent to reveal confidential information, the inquirer must not reveal confidential information regarding the representation, but must only respond in a general way, such as that the inquirer disagrees with the client's statements. The inquirer should not disclose that the court entered an order allowing the inquirer to withdraw because that is information relating to the client's representation and the client did not give informed consent for the inquirer to disclose.

The inquirer refers to Texas Ethics Opinion 622. That opinion explains that a lawyer may not respond to client's negative internet review if the response discloses confidential information. The opinion gives an example of a proportional and restrained response that does not reveal any confidential information:

> A lawyer's duty to keep client confidences has few exceptions and in an abundance of caution I do not feel at liberty to respond in a point by point fashion in this forum. Suffice it to say that I do not believe that the post presents a fair and accurate picture of the events.

The suggested language found in Texas Ethics Opinion 622 would be an acceptable response for the inquirer. The inquirer also may state that the inquirer disagrees with the facts stated in the review in an alternative response as follows:

> As an attorney, I am constrained by the Rules Regulating The Florida Bar from responding in detail, but I will simply state that it is my belief that the [comments/post] present neither a fair nor accurate picture of what occurred and I believe that the [comments/post] [is/are] false.

FLORIDA BAR ETHICS OPINION
OPINION 14-1
June 25, 2015

Advisory ethics opinions are not binding.

A personal injury lawyer may advise a client pre-litigation to change privacy settings on the client's social media pages so that they are not publicly accessible. Provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, the lawyer also may advise that a client remove information relevant to the foreseeable proceeding from social media pages as long as the social media information or data is preserved.

Note: This opinion was approved by The Florida Bar Board of Governors on October 16, 2015.

RPC: 4-3.4(a)
Opinions: New York County Ethics Opinion 745; North Carolina Formal Ethics Opinion 5; Pennsylvania Bar Association Opinion 2014-300; Philadelphia Bar Association Professional Guidance Committee Opinion 2014-5
Cases: *Allied Concrete Co. v. Lester,* 736 S.E.2d 699 (Va. 2013); *Gatto v. United Airlines,* 2013 WL 1285285, Case No. 10-cv-1090-ES-SCM (U.S. Dist. Ct. NJ March 25, 2013); *In the Matter of Matthew B. Murray,* 2013 WL 5630414, VSB Docket Nos. 11-070-088405 and 11-070-088422 (Virginia State Bar Disciplinary Board July 17, 2013); *Romano v. Steelcase, Inc.* 907 N.Y.S.2d 650 (NY 2010); *Root v. Balfour Beatty Construction, Inc.,*132 So.3d 867, 869-70 (Fla. 2nd DCA 2014)
Misc.: Guideline No. 4.A, Social Media Ethics Guidelines, New York State Bar Association's Commercial and Federal Litigation Section

A Florida Bar member who handles personal injury and wrongful death cases has asked the committee regarding the ethical obligations on advising clients to "clean up" their social media pages before litigation is filed to remove embarrassing information that the lawyer believes is not material to the litigation matter. The inquirer asks the following 4 questions:

1) Pre-litigation, may a lawyer advise a client to remove posts, photos, videos, and information from social media pages/accounts that are related directly to the incident for which the lawyer is retained?

2) Pre-litigation, may a lawyer advise a client to remove posts, photos, videos, and information from social media pages/accounts that are not related directly to the incident for which the lawyer is retained?

3) Pre-litigation, may a lawyer advise a client to change social media pages/accounts privacy settings to remove the pages/accounts from public view?

4) Pre-litigation, must a lawyer advise a client not to remove posts, photos, videos and information whether or not directly related to the litigation if the lawyer has advised the client to set privacy settings to not allow public access?

Rule 4-3.4(a) is applicable and states as follows:

A lawyer must not:

(a) unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act;

The comment to the rule provides further guidance:

The procedure of the adversary system contemplates that the evidence in a case is to be marshalled competitively by the contending parties. Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like.

Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed, or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for the purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense. Subdivision (a) applies to evidentiary material generally, including computerized information.

Under these facts, the proper inquiry is whether information on a client's social media page is relevant to a "reasonably foreseeable proceeding," rather than whether information is "related directly" or "not related directly" to the client's matter. Information that is not "related directly" to the incident giving rise to the need for legal representation may still be relevant. However, what is relevant requires a factual, case-by-case determination. In Florida, the second District Court of Appeal has determined that normal discovery principles apply to social media, and that information sought to be discovered from social media must be "(1) relevant to the case's subject matter, and (2) admissible in court or reasonably calculated to lead to evidence that is admissible in court." *Root v. Balfour Beatty Construction, Inc.,*132 So.3d 867, 869-70 (Fla. 2nd DCA 2014).

What constitutes an "unlawful" obstruction, alteration, destruction, or concealment of evidence is a legal question, outside the scope of an ethics opinion. The committee is aware of cases addressing the issue of discovery or spoliation relating to social media, but in these cases, the issue arose in the course of discovery after litigation commenced. *See, Allied Concrete Co. v. Lester,* 736 S.E.2d 699 (Va. 2013) (Sanctions of $542,000 imposed against lawyer and $180,000 against the client for spoliation when client, at lawyer's direction, deleted photographs from

client's social media page, the client deleted the accounts, and the lawyer signed discovery requests that the client did not have the accounts); *Gatto v. United Airlines,* 2013 WL 1285285, Case No. 10-cv-1090-ES-SCM (U.S. Dist. Ct. NJ March 25, 2013) (Adverse inference instruction, but no monetary sanctions, against plaintiff who deactivated his social media accounts, which then became unavailable, after the defendants requested access); *Romano v. Steelcase, Inc.* 907 N.Y.S.2d 650 (NY 2010) (Court granted request for access to plaintiff's MySpace and Facebook pages, including private and deleted pages, when plaintiff's physical condition was at issue and information on the pages is inconsistent with her purported injuries based on information about plaintiff's activities available on the public pages of her MySpace and Facebook pages). In the disciplinary context, at least one lawyer has been suspended for 5 years for advising a client to clean up the client's Facebook page, causing the removal of photographs and other material after a request for production had been made. *In the Matter of Matthew B. Murray,* 2013 WL 5630414, VSB Docket Nos. 11-070-088405 and 11-070-088422 (Virginia State Bar Disciplinary Board July 17, 2013).

The New York County Lawyers Association has issued NYCLA Ethics Opinion 745 (2013) addressing the issue. The opinion concludes that lawyers may advise their clients to use the highest level of privacy settings on their social media pages and may advise clients to remove information from social media pages unless the lawyer has a duty to preserve information under law and there is no violation of law relating to spoliation of evidence. Other states have since come to similar conclusions. See, e.g., North Carolina Formal Ethics Opinion 5 (attorney must advise client about information on social media if information is relevant and material to the client's representation and attorney may advise client to remove information on social media if not spoliation or otherwise illegal); Pennsylvania Bar Association Opinion 2014-300 (attorney may advise client to delete information from client's social media provided that this does not constitute spoliation or is otherwise illegal, but must take appropriate action to preserve the information); and Philadelphia Bar Association Professional Guidance Committee Opinion 2014-5 (attorney may advise a client to change the privacy settings on the client's social media page but may not instruct client to destroy any relevant content on the page). Subsequent to the publication of the opinion, the New York State Bar Association's Commercial and Federal Litigation Section adopted Social Media Ethics Guidelines. Guideline No. 4.A, citing to the opinion, states as follows:

> A lawyer may advise a client as to what content may be maintained or made private on her social media account, as well as to what content may be "taken down" or removed, whether posted by the client or someone else, as long as there is no violation of common law or any statute, rule, or regulation relating to the preservation of information. Unless an appropriate record of the social media information or data is preserved, a party or nonparty may not delete information from a social media profile that is subject to a duty to preserve. [Footnote omitted.]

The committee agrees with the NYCLA that a lawyer may advise a client to use the highest level of privacy setting on the client's social media pages.

The committee also agrees that a lawyer may advise the client pre-litigation to remove information from a social media page, regardless of its relevance to a reasonably foreseeable

proceeding, as long as the removal does not violate any substantive law regarding preservation and/or spoliation of evidence. The committee is of the opinion that if the inquirer does so, the social media information or data must be preserved if the information or data is known by the inquirer or reasonably should be known by the inquirer to be relevant to the reasonably foreseeable proceeding.

The committee is of the opinion that the general obligation of competence may require the inquirer to advise the client regarding removal of relevant information from the client's social media pages, including whether removal would violate any legal duties regarding preservation of evidence, regardless of the privacy settings. If a client specifically asks the inquirer regarding removal of information, the inquirer's advice must comply with Rule 4-3.4(a). What information on a social media page is relevant to reasonably foreseeable litigation is a factual question that must be determined on a case-by-case basis.

In summary, the inquirer may advise that a client change privacy settings on the client's social media pages so that they are not publicly accessible. Provided that there is no violation of the rules or substantive law pertaining to the preservation and/or spoliation of evidence, the inquirer also may advise that a client remove information relevant to the foreseeable proceeding from social media pages as long as the social media information or data is preserved.

FLORIDA BAR ETHICS OPINION
OPINION 12-3
January 25, 2013

Advisory ethics opinions are not binding.

Lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.

Note: This opinion was affirmed by the Board of Governors with slight modification on July 26, 2013.

RPC: 4-1.6
Opinions: 10-2, 07-2, Alabama 2010-02, Arizona 09-04, Iowa 11-01, Nevada 33, New York State 842, Pennsylvania 2011-200

The Professional Ethics Committee has been directed by The Florida Bar Board of Governors to issue an opinion regarding lawyers' use of cloud computing. "Cloud computing" is defined as "Internet-based computing in which large groups of remote servers are networked so as to allow sharing of data-processing tasks, centralized data storage, and online access to computer services or resources."1 It is also defined as "A model of computer use in which services stored on the internet are provided to users on a temporary basis."2 Because cloud computing involves the use of a third party as a provider of services and involves the storage and use of data at a remote location that is also used by others outside an individual law firm, the use of cloud computing raises ethics concerns of confidentiality, competence, and proper supervision of nonlawyers.

In other words, cloud computing involves use of an outside service provider which provides computing software and data storage from a remote location that the lawyer accesses over the Internet via a web browser, such as Internet Explorer, or via an "app" on smart phones and tablets. The lawyer's files are stored at the service provider's remote server(s). The lawyer can thus access the lawyer's files from any computer or smart device and can share files with others. Software is purchased, maintained, and updated by the service provider. Many lawyers and others are computing "in the cloud" because of convenience and potential cost savings.

The main concern regarding cloud computing relates to confidentiality. Lawyers have an obligation to maintain as confidential all information that relates to a client's representation, regardless of the source. Rule 4-1.6, Rules Regulating The Florida Bar. A lawyer may not voluntarily disclose any information relating to a client's representation without either

---

1 *Collins English Dictionary - Complete & Unabridged 10th Edition*. HarperCollins Publishers. 10 Sep. 2012. <Dictionary.com http://dictionary.reference.com/browse/cloud computing>.

2 *Id.*

application of an exception to the confidentiality rule or the client's informed consent. *Id.* A lawyer has the obligation to ensure that confidentiality of information is maintained by nonlawyers under the lawyer's supervision, including nonlawyers that are third parties used by the lawyer in the provision of legal services. *See,* Florida Ethics Opinion 07-2 and 10-2.

Additionally, this Committee has previously opined that lawyers have an obligation to remain current not only in developments in the law, but also developments in technology that affect the practice of law. Florida Ethics Opinion 10-2. Lawyers who use cloud computing therefore have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations.

Other states that have addressed the issue of cloud computing have generally determined that there are ethics concerns regarding confidentiality of information, but that a lawyer may compute via the cloud if the lawyer takes reasonable steps. *See, e.g.,* Alabama Ethics Opinion 2010-02 (Lawyer may outsource storage of client files through cloud computing if they take reasonable steps to make sure data is protected); Arizona Ethics Opinion 09-04 (2009) (Lawyer may use online file storage and retrieval system that enables clients to access their files over the Internet, as long as the firm takes reasonable precautions to protect confidentiality of the information); Iowa Ethics Opinion 11-01 (2011) (Appropriate due diligence a lawyer should perform before storing files electronically with a third party using SaaS (cloud computing), includes determining that the lawyer will have adequate access to the stored information, the lawyer will be able to restrict access of others to the stored information, whether data is encrypted and password protected, and what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider); Nevada Formal Ethics Opinion 33 (2006) (Attorney may store client files electronically on a remote server controlled by a third party as long as the firm takes precautions to safeguard confidential information such as obtaining the third party's agreement to maintain confidentiality); New York State Bar Ethics Opinion 842 (2010) (Lawyer may use an online computer data storage system to store client files provided the attorney takes reasonable care to maintain confidentiality, and the lawyer must stay informed of both technological advances that could affect confidentiality and changes in the law that could affect privilege); and Pennsylvania Ethics Opinion 2011-200 ("An attorney may ethically allow client confidential material to be stored in 'the cloud' provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks").

This Committee agrees with the opinions issued by the states that have addressed the issue. Cloud computing is permissible as long as the lawyer adequately addresses the potential risks associated with it. As indicated by other states that have addressed the issue, lawyers must perform due diligence in researching the outside service provider(s) to ensure that adequate safeguards exist to protect information stored by the service provider(s). New York State Bar Ethics Opinion 842 suggests the following steps involve the appropriate due diligence:

- 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;

- Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

Of particular practical assistance is Iowa Ethics Opinion 11-01. As suggested by the Iowa opinion, lawyers must be able to access the lawyer's own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third parties to specific information, yet must be able to restrict their access to only that information. Iowa Ethics Opinion 11-01 also recommends considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which any dispute will be decided, whether it limits the service provider's liability, whether the service provider retains the information in the event the lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the service provider, and whether the agreement creates "any proprietary or user rights" over the data the lawyer stores with the service provider. It also suggests that the lawyer determine whether the information is password protected, whether the information is encrypted, and whether the lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a particular matter or piece of information. It further suggests that the lawyer consider whether the information stored via cloud computing is also stored elsewhere by the lawyer in the event the lawyer cannot access the information via "the cloud."

This Committee agrees with the advice given by both Iowa and New York State. Additionally, this Committee believes that the lawyer should consider whether the lawyer should use the outside service provider or use additional security in specific matters in which the lawyer has proprietary client information or has other particularly sensitive information.

In summary, lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. The lawyer should research the service provider to be used.

FLORIDA BAR ETHICS OPINION
OPINION 10-2
September 24, 2010

Advisory ethics opinions are not binding.

A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

RPC: 4-1.1, 4-1.6(a), 4-5.3(b)

The Professional Ethics Committee has been asked by the Florida Bar Board of Governors to write an opinion addressing the ethical obligations of lawyers regarding information stored on hard drives. An increasing number of devices such as computers, printers, copiers, scanners, cellular phones, personal digital assistants ("PDA's"), flash drives, memory sticks, facsimile machines and other electronic or digital devices (collectively, "Devices") now contain hard drives or other data storage media[1] (collectively "Hard Drives" or "Storage Media") that can store information.[2] Because many lawyers use these Devices to assist in the practice of law and in doing so intentionally and unintentionally store their clients' information on these Devices, it is important for lawyers to recognize that the ability of the Devices to store information may present potential ethical problems for lawyers.

For example, when a lawyer copies a document using a photocopier that contains a hard drive, the document is converted into a file that is stored on the copier's hard

---

1 As used in this opinion, Storage Media is any media that stores digital representations of documents.

2 *See* Brian Smithson, *The IEEE 2600 Series: An Introduction to New Security Standards for Hardcopy* Devices, ISSA JOURNAL, Nov. 2009, at 28; Holly Herman, *Experts Warn Copiers Can Be Fertile Ground for ID Thieves*, READING EAGLE (Jun. 2, 2010, 12:28:54 P.M.), http://readingeagle.com/article.aspx?id=222523; Mark Huffman, *Digital Copiers Could Be an Identity Theft Threat*, ConsumerAffairs.com (May 19, 2010), http://www.consumeraffairs.com/news04/2010/05/digital_copiers.html; Armen Keteyian, *Digital Photocopiers Loaded with Secrets*, CBSNews.com (April 15, 2010), http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml; Gregg Kelzer, *Photocopiers: The Newest ID Theft Threat*, COMPUTERWORLD (March 14, 2007), http://www.computerworld.com/s/article/9013104/Photocopiers_The_newest_ID_theft_threat.

drive. This document usually remains on the hard drive until it is overwritten or deleted. The lawyer may choose to later sell the photocopier or return it to a leasing company. Disposal of the device without first removing the information can result in the inadvertent disclosure of confidential information.

Duty of Confidentiality

Lawyers have an ethical obligation to protect information relating to the representation of a client. Rule 4-1.6(a) of the Rules Regulating the Florida Bar addresses the duty of confidentiality and states:

> **(a) Consent Required to Reveal Information.** A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.

The comment to the rule further states:

> The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or by law.

A lawyer must ensure confidentiality by taking reasonable steps to protect all confidential information under the lawyer's control. Those reasonable steps include identifying areas where confidential information could be potentially exposed. Rule 4-1.1 addresses a lawyer's duty of competence:

> **Competence** A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

The comment to the rule further elaborates:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law *and its practice*, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.

(emphasis added).

If a lawyer chooses to use these Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality. The lawyer must learn such details as whether the Device has the ability to store confidential information, whether the information can be accessed by unauthorized parties, and who can potentially have access to the information. The lawyer must also be aware of different environments in which confidential information is exposed such as public copy centers, hotel business centers,

and home offices. The lawyer should obtain enough information to know when to seek protection and what Devices must be sanitized, or cleared of all confidential information, before disposal or other disposition. Therefore, the duty of competence extends from the receipt, i.e., when the lawyer obtains control of the Device, through the Device's life cycle, and until disposition of the Device, including after it leaves the control of the lawyer. Further, while legal matters are beyond the scope of an ethics opinion, a lawyer should be aware that depending on the nature of the information, misuse of these Devices could result in inadvertent violation of state and federal statutes governing the disclosure of sensitive personal information such as medical records, social security numbers, criminal arrest records, etc.

Duty to Supervise

The lawyer must regulate not only the lawyer's own conduct but must take reasonable steps to ensure that all nonlawyers over whom the lawyer has supervisory responsibility adhere to the duty of confidentiality as well. Rule 4-5.3(b) states:

> **(b) Supervisory Responsibility.** With respect to a nonlawyer employed or retained by or associated with a lawyer or an authorized business entity as defined elsewhere in these Rules Regulating The Florida Bar:
>
> (1) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (2) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (3) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (A) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (B) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

A lawyer's supervisory responsibility extends not only to the lawyer's own employees but over entities outside the lawyer's firm with whom the lawyer contracts to assist in the care and maintenance of the Devices in the lawyer's control. If a nonlawyer

will have access to confidential information, the lawyer must obtain adequate assurances from the nonlawyer that confidentiality of the information will be maintained.

Sanitization

A lawyer has a duty to obtain adequate assurances that the Device has been stripped of all confidential information before disposition of the Device. If a vendor or other service provider is involved in the sanitization of the Device, such as at the termination of a lease agreement or upon sale of the Device, it is not sufficient to merely obtain an agreement that the vendor will sanitize the Device upon sale or turn back of the Device. The lawyer has an affirmative obligation to ascertain that the sanitization has been accomplished, whether by some type of meaningful confirmation, by having the sanitization occur at the lawyer's office, or by other similar means.

Further, a lawyer should use care when using Devices in public places such as at copy centers, hotel business centers, and outside offices where the lawyer and those under the lawyer's supervision have little or no control. In such situations, the lawyer should inquire and determine whether use of such Devices would preserve confidentiality under these rules.

In conclusion, when a lawyer chooses to use Devices that contain Storage Media, the lawyer must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition. These reasonable steps include: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

FLORIDA BAR ETHICS OPINION
OPINION 07-1
September 7, 2007

Advisory ethics opinions are not binding.

A lawyer whose client has provided the lawyer with documents that were wrongfully obtained by the client may need to consult with a criminal defense lawyer to determine if the client has committed a crime. The lawyer must advise the client that the materials cannot be retained, reviewed or used without informing the opposing party that the inquiring attorney and client have the documents at issue. If the client refuses to consent to disclosure, the inquiring attorney must withdraw from the representation.

RPC: 4-1.2(d), 4-1.4, 4-1.6, 4-1.16(a)(1), 4-3.4(a), 4-4.4(a), 4-4.4(b), 4-8.4(a), 4-8.4(c), 4-8.4(d)

Opinions: 93-3; ABA Formal Opinion 94-382; ABA Formal Opinion 06-440; ABA Formal Opinion 05-437; Connecticut Opinion 96-4; New Jersey Opinion 680; New York City Opinion 1989-1

Cases: *Anderson v. State*, 297 So.2d 871 (Fla. 2d DCA 1974); *Florida Bar v. Hmielewski*, 702 So.2d 218 (Fla. 1997); *Moldonado v. New Jersey, Administrative Office of the Courts - Probation Division*, 225 F.R.D. 120 (D. N.J. 2004); *Perna v. Electronic Data Systems, Corporation*, 916 F.Supp. 388 (D.N.J. 1995); *Quinones v. State*, 766 So.2d 1165 (Fla. 3d DCA 1974)

A member of The Florida Bar has requested an advisory ethics opinion. The operative facts as presented in the inquiring attorney's letter are as follows:

> I represent the petitioner/wife in a dissolution of action currently pending in [local county], Florida. Wife maintains a small professional space within an office owned by a company in which her husband is a 50% shareholder. Prior to separation of the parties, wife frequently utilized husband's corporate office space for printing, copying, computer use, etc. Since separation, wife is no longer welcome to use these amenities unsupervised or after hours. It has come to my attention that my client has done the following: (1) Removed documents from husband's office prior to and after separation; (2) Figured out husband's computer and e-mail password and, at his office, printed off certain documents, including financial documents of the corporation, husband's personal documents and e-mails with third parties of a personal nature, and documents or e-mails authored by husband's attorney in this action; (3) Accessed husband's personal e-mail from wife's home computer, and printed and downloaded confidential or privileged documents; and (4) despite repeated warning of the wrongfulness of wife's past conduct by this office, removed documents from husband's car which are believed to be attorney-client privileged.
>
> Wife has produced to my office certain documents listed in 1-3 above, which production alerted me to this issue. This office has not reviewed those documents

believed to contain attorney-client privileged information and immediately segregated those documents and any copies in a sealed envelope. Wife claims that she is not in possession of any other documents subject to 1-3 above, and that she did not review those that contain reference to husband's attorney.

I believe documents removed from husband's car referenced in 4 above, which may be attorney-client privileged, are in the custody of wife, who claims she has not reviewed the document, but contacted counsel upon discovery of potentially confidential material.

I have reviewed the Florida and ABA opinions and contacted the Florida Bar Hotline. It does not appear that any cases specifically address obligations of disclosure to opposing counsel wherein one party obtained the documents in a potentially illegal manner. The cases appear to be limited to cases of inadvertent disclosure by the revealing party. I am unsure of my obligation of disclosure and/or to return the documents to husband's counsel without violating my obligation of confidentiality and representation to my client, and request a written staff opinion regarding same.

Discussion

Rule 4-4.4(b) provides that "[a] lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." In an opinion predating the adoption of Rule 4-4.4(b), Florida Ethics Opinion 93-3, this committee came to the same conclusion.

However, the instant facts are distinguishable from the typical scenario involving inadvertent disclosure of privileged documents. There was no inadvertent disclosure. Rather, the materials were deliberately obtained by inquiring attorney's client without the permission of the opposing party. The comment to Rule 4-4.4(b) mentions such situations, but does not provide substantial guidance:

> Subdivision (b) recognizes that lawyers sometimes receive documents that were mistakenly sent or produced by opposing parties or their lawyers. If a lawyer knows or reasonably should know that such a document was sent inadvertently, then this rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these rules, as is the question of whether the privileged status of a document has been waived. *Similarly, this rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person*. For purposes of this rule, "document" includes e-mail or other electronic modes of transmission subject to being read or put into readable form.
>
> Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the

> wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer. See rules 4-1.2 and 4-1.4.

(emphasis added).

The American Bar Association formerly had an ethics opinion addressing a lawyer's duties when the lawyer receives confidential information from someone who is not authorized to release the information. In Formal Opinion 94-382, the ABA Standing Committee on Ethics and Professional Responsibility determined that an attorney who receives an adverse party's confidential materials from someone who is not authorized to disclose them should refrain from reviewing the materials and either contact opposing counsel for instructions or seek a court order allowing the recipient to use them. The ABA recently withdrew that opinion in Formal Opinion 06-440, deciding that Opinion 94-382 was not supported by the rules, especially ABA Model Rule 4.4(b) which is the equivalent of Florida Rule 4-4.4(b). Specifically, the ABA committee stated:

> As was noted in Formal Opinion 05-437, Rule 4.4(b) requires only that a lawyer who receives a document relating to the representation of the lawyer's client and who knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender. The Rule does not require refraining from reviewing the materials or abiding by instructions of the sender. Thus, even assuming that the materials sent intentionally but without authorization could be deemed "inadvertently sent" so that the subject is one addressed by Rule 4.4(b), the instructions of Formal Opinion 94-382 are not supported by the Rule.
>
> It further is our opinion that if the providing of the materials is not the result of the sender's inadvertence, Rule 4.4(b) does not apply to the factual situation addressed in Formal Opinion 94-382. A lawyer receiving materials under such circumstances is therefore not required to notify another party or that party's lawyer of receipt as a matter of compliance with the Model Rules. Whether a lawyer may be required to take any action in such an event is a matter of law beyond the scope of Rule 4.4(b).
>
> Accordingly, because the advice presented in Formal Opinion 94-382 is not supported by the Rules, the opinion is withdrawn in its entirety.

Therefore, neither Rule 4-4.4(b) nor Opinion 93-3 directly govern the inquiring attorney's situation.

The Comment to Rule 4-4.4(b) states that the rule does not address the legal duties of a lawyer who receives documents that were wrongfully obtained. Similarly, under the Florida Bar Procedures For Ruling on Questions of Ethics it is beyond the scope of an advisory ethics opinion for this committee to resolve legal issues, such as whether the inquiring attorney has a legal duty (independent of any duty the client may have) to return the documents to their owner. Nor can this opinion resolve the legal question of whether the client's conduct violated any criminal laws. However, to merely refer the inquiring attorney to the comment to Rule 4-4.4(b)

and point out that there are legal issues to be resolved does a disservice to the inquiring attorney. While there are legal issues that this committee cannot resolve, there is ethical guidance that can be provided. Further, for the purposes of this guidance, it will be presumed that, whether or not the client's conduct was illegal, it was improper. If the client's conduct was rightful and proper the inquiring attorney would not be seeking guidance.

While Rule 4-4.4(b) does not govern the inquiring attorney's quandary, other rules are applicable. One such rule is Rule 4-1.6, the ethical duty of confidentiality. This rule states, in part:

> **(a) Consent Required to Reveal Information.** A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.
>
> **(b) When Lawyer Must Reveal Information.** A lawyer shall reveal such information to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent a client from committing a crime; or
>
> (2) to prevent a death or substantial bodily harm to another.
>
> **(c) When Lawyer May Reveal Information.** A lawyer may reveal such information to the extent the lawyer reasonably believes necessary:
>
> (1) to serve the client's interest unless it is information the client specifically requires not to be disclosed;
>
> (2) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and client;
>
> (3) to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved;
>
> (4) to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
>
> (5) to comply with the Rules of Professional Conduct.

The confidentiality rule makes any information relating to the representation of a client confidential, *whatever the source*. Comment, Rule 4-1.6. It is broader than the attorney-client privilege. Thus, under the rule, an attorney cannot voluntarily reveal any information relating to the representation of a client unless the client consents or an exception to the rule is applicable.

Another rule that is applicable to the inquiring attorney's situation is Rule 4-3.4(a). This rule states:

> A lawyer shall not:

(a) unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act;

Still other rules are applicable. Rule 4-4.4(a) prohibits a lawyer from knowingly using "methods of obtaining evidence that violate the legal rights" of third persons. Rule 4-1.2(d) prohibits a lawyer from assisting a client in conduct that the lawyer knows or reasonably should know is criminal or fraudulent. Rule 4-1.4 requires lawyers to fully advise clients. Rule 4-8.4(d) prohibits lawyers from engaging in conduct that is prejudicial to the administration of justice. Rule 4-8.4(a) prohibits a lawyer from violating the rules through the acts of another.

Additionally, while there is no formal opinion in Florida providing guidance in a situation such as that facing the inquiring attorney, there is at least one disciplinary case that touches on the issues presented by the inquiring attorney. In *The Florida Bar v. Hmielewski*, 702 So. 2d 218 (Fla. 1997) an attorney represented a client in a wrongful death claim alleging medical malpractice arising from the death of the client's father. After the attorney was retained, but before suit was filed, the client told the attorney that he had taken some of his father's medical records from the hospital involved and showed the attorney the records. In discovery, the attorney asked the hospital to produce the records, which it could not. The hospital, in its own discovery request, asked for the production of any medical records the client had. The attorney did not disclose the records. The attorney stated to the court that one of the issues in the case was the hospital's failure to maintain the records, the attorney submitted an expert report that the hospital tampered with its medical records even though the attorney knew the expert's opinion was based on the expert's belief that the hospital failed to maintain the records, and made other misrepresentations. After the fact that the client took the records came out during the client's deposition, the court sanctioned the client and the attorney and filed a bar complaint against the attorney.

The Florida Supreme Court upheld the referee's findings based on the above facts:

The referee recommended that Hmielewski be found guilty of violating the following Rules Regulating The Florida Bar: (1) rule 3-4.3, which proscribes conduct that is unlawful or contrary to honesty or justice; (2) rule 4-3.3(a)(1), which prohibits knowingly making false statements of material fact or law to a tribunal; (3) rule 4-3.3(a)(2), which prohibits failing to disclose a material fact to a tribunal when disclosure is necessary to avoid assisting a criminal or fraudulent act by the client; (4) rule 4-3.4(a), which prohibits both the unlawful obstruction of another party's access to evidence and the unlawful altering, destruction or concealment of a document or other material that the lawyer knows or reasonably should know is relevant to a pending or reasonably foreseeable proceeding, or counseling or assisting another person to do such an act; (5) rule 4-3.4(d), which prohibits the intentional failure to comply with legally proper discovery requests; (6) rule 4-4.1(a), which mandates that lawyers not make false statements of material fact or law to third persons while representing a client; (7) rule 4-4.4, which prohibits the use of methods of obtaining evidence that violate the rights of

third persons; and (8) rule 4-8.4(c), which prohibits conduct involving dishonesty, fraud, deceit, or misrepresentation.

The referee recommended that Hmielewski be suspended from the practice of law for one year followed by two years of probation, noting that the character and reputation testimony presented on Hmielewski's behalf was the primary mitigating factor that saved Hmielewski from disbarment.

"A referee's findings of fact carry a presumption of correctness that should be upheld unless clearly erroneous or without support in the record." *Florida Bar v. Berman, 659 So.2d 1049, 1050 (Fla.1995)*. We find support in the record for the referee's factual findings. These findings establish that Hmielewski improperly allowed what he perceived as his duty to his client to overshadow his duty to the justice system when he made deliberate misrepresentations of material fact to the Mayo Clinic and the Minnesota trial court. Hmielewski's violations made a mockery of the justice system and flew in the face of Hmielewski's ethical responsibilities as a member of The Florida Bar.

702 So. 2d at 220. The court suspended the attorney for three years.

Clearly, under *Hmielewski*, the inquiring attorney cannot make any misrepresentations about the documents, including in response to any discovery requests regarding the documents. Nor can the inquiring attorney make the documents, including the opponent's failure to produce them or have them in his custody, a feature of the case without disclosing that the inquirer has the documents. However, *Hmielewski* did not address what the attorney should have done when the attorney first learned that the client obtained the documents.

Other jurisdictions also have addressed the issue of a lawyer's responsibilities when the lawyer's client improperly gets confidential or privileged documents of the opposing party. Connecticut Opinion 96-4 states that an attorney whose client improperly obtained a release of the client's spouse's medical records may not permit the client to copy or view the records and must return the records to the records custodian unless a proper release is signed. New Jersey Opinion 680 (1995) dealt with a situation where opposing counsel came to the work place of another attorney's clients to examine documents during discovery. When both opposing counsel and the client's own attorney took a lunch break, the client went through a stack of the opposing attorney's papers and made copies of them. When the attorney was told of the client's action, he sought the ethics opinion. The attorney did not come into possession of any of the documents. As stated in the New Jersey opinion:

The nub of the problem posed by the inquiry lies with the fact that the clients gained access, without permission, to private, confidential documents of adversaries in litigation. Two of the principals of the client are not in accord as to the precise circumstances by which this access was gained, but in any event it was unauthorized.

No Rule of Professional Conduct directly deals with this specific situation, nor does any prior opinion of this Committee. Neither RPC 3.4 (Fairness to Opposing

> Party and Counsel) nor RPC 4.1 (Truthfulness in Statements to Others) clearly and directly reaches the situation posed by the inquirer. Further, while under RPC 4.1(a)(2) in some circumstances a client's seizure of evidence in the hands of an adversary certainly could constitute "a criminal or fraudulent act," we do not have enough evidence to draw such a conclusion here. Similarly, on the facts presented, the lawyer did not "use methods of obtaining evidence that violate the legal rights of such a [third] person," under RPC 4.4, as the actions were taken by a client.
>
> Nonetheless, the client's reading of the adversary's documents was distinctly inappropriate and improper, constituting a clear invasion of privacy at the very least. If the lawyer had committed the acts ascribed to the clients, and items of evidence were involved, it would constitute a violation of RPC 4.4. It is well established that an attorney may not do indirectly that which is prohibited directly (see RPC 8.4(a)), and consequently the lawyer cannot be involved in the subsequent review of evidence obtained improperly by the client. Furthermore, the conduct of inquirer's client may have been of benefit to that client in the litigation. For a lawyer to allow a client's improper actions taken in the context of litigation to benefit that client in such litigation would constitute "conduct that is prejudicial to the administration of justice" under RPC 8.4(d). Only disclosure to the adversary will avoid the prejudicial effect proscribed by this rule, and thus this situation falls within those in which disclosure of confidential information is permitted by RPC 1.6(c)(3) in order "to comply with other law." Mere withdrawal from representation, without disclosure, will not reverse the prejudicial conduct.

The incident that formed the basis of New Jersey Opinion 680 is also the subject of *Perna v. Electronic Data Systems, Corporation*, 916 F. Supp 388 (D. N.J. 1995). In that case, the court sanctioned the partner who viewed and copied the opposing parties documents by dismissing the partner's individual claims. Of the conduct of the partner's attorneys, the Court noted that the attorneys did not engage in any misconduct and applauded their decision to seek ethical guidance. 916 F.Supp at 394, footnote 5.

In another case from New Jersey, *Maldonado v. New Jersey, Administrative Office of the Courts –Probation Division*, 225 F.R.D. 120 (D. N.J. 2004), a plaintiff who was employed as a probation officer filed a discrimination lawsuit against his employer and two individual probation officers. Prior to the lawsuit, the plaintiff filed an administrative claim with the New Jersey Division on Civil Rights (NJDCR). The NJDCR proceeding resulted in a finding of probable cause. The two individual probation officers named wrote a letter on October 7, 2001 to their attorney regarding the credibility of the witnesses interviewed in the NJDCR matter. At a later date in 2001, a copy of the letter came into the possession of the plaintiff. The plaintiff claimed someone put it in his workplace mailbox. The defendants suspected that the plaintiff took it from one of the individual defendant's office, but were unable to prove this. The plaintiff gave the copy of the letter to his attorneys. Information from the letter was used by the attorneys in the original civil complaint filed in October 2003. However, defense counsel did not notice this until the amended complaint was reviewed in a meeting between plaintiff and defense counsel in the spring of 2004. Defense counsel then filed a motion for protective order, to

dismiss the plaintiff's complaint as a sanction or alternatively to disqualify the plaintiff's attorneys.

The court found that under the circumstances, the attorney client and work product privileges were not waived. The court further declined to dismiss the plaintiff's case, in part because it was not proven that the plaintiff intentionally took the letter. However, the Court did order the disqualification of the plaintiff's attorneys:

> In sum, the record before the Court shows the following: 1) Maldonado's present counsel had access to privileged material since at least October 3, 2003; 2) counsel reviewed and relied on the October 7th letter in formulating Maldonado's case; 3) the letter was highly relevant and prejudicial to Defendants' case; 4) counsel did not adequately notify opposing counsel of their possession of the material; 5) Defendants took reasonable precautions to protect the letter and cannot be found at fault for the disclosure; and 6) Maldonado would not be severely prejudiced by the loss of his counsel of choice.
>
> * * *
>
> Both Matos and Hodulik did not adhere to the "cease, notify, and return" mandate of the New Jersey Supreme Court's Advisory Committee on Professional Ethics [Opinion 680] and the New Jersey Rules of Professional Conduct. The Court's decision, however, rests more appropriately on the prejudicial effect that the disclosure of the October 7th letter has on Defendants' case. This sanction is drastic; yet, in disqualification situations any doubt is to be resolved in favor of disqualification. Therefore, the Court finds that the appropriate remedy to mitigate the prejudicial effects of counsels' possession, review,*142 and use of the letter is the disqualification of Matos and Hodulik.
>
> 225 F.R.D. at 141-142.

The Association of the Bar of the City of New York in its Ethics Opinion1989-1 addressed the issue of an attorney's obligations when a spouse in a matrimonial case intercepted communications between the other spouse and that spouse's attorney. The New York Committee came to a somewhat different conclusion than New Jersey, based on the duty of confidentiality to the client:

> Where the inquirer has not suggested or initiated the practice in any way, the question to be resolved is whether any ethical obligations or prohibitions constrain the inquiring attorney's use of the copied communications. The Committee concludes that, regardless of whether the lawyer counseled the client to engage in this conduct or even knew that the client was so engaged, it would be unethical for the lawyer to use any intercepted communications to advance the client's position unless and until the lawyer (i) has disclosed to adversary counsel the fact that the documents have come into the lawyer's possession and (ii) has provided copies to adversary counsel. Even if the lawyer does not intend to make affirmative use of the documents, the lawyer must promptly disclose his

possession of the documents and return them or copies of them. *Because the intercepted communications were received by the lawyer in the course of the professional relationship, however, the lawyer may not make such disclosure without the consent of the client. DR 4-101(B). If the client refuses to permit disclosure or the return of the documents to the adversary, the lawyer must withdraw from the representation. DR 2-110(B).*

(Emphasis added).

Application to the Inquiring Attorney's Query

The inquiring attorney is in possession of certain categories of documents that the client either (1) removed from the husband's office, (2) printed from the husband's computer, including financial documents and emails, or (3) accessed on her own computer with the husband's password. The inquiring attorney segregated and has not reviewed any documents that the inquirer believes contain attorney-client privileged information. By implication, this means the inquiring attorney has reviewed documents that the inquirer believed not to be privileged.

Additionally, the inquiring attorney also states that the client removed documents from the husband's vehicle, and that the inquiring attorney believes these documents are privileged. The inquiring attorney is not in possession of this latter category of documents. Rather, the client has them and says she has not reviewed the documents.

As noted earlier in the opinion, this Committee is not authorized to decide questions of law, including whether the inquiring attorney has a duty to return or disclose the documents in the inquirer's possession. However, there can be circumstances where a lawyer would have an obligation under the law to return or disclose the documents. For instance, a lawyer would have to produce the documents in response to a valid discovery request for the documents. *See* Rule 4-3.4(d) (prohibits intentional failure to comply with legally proper discovery requests) and *The Florida Bar v. Hmielewski*, 702 So. 2d 218 (Fla. 1997). If the documents themselves were stolen property, the lawyer may also have an obligation under substantive law to turn over the documents. *See Quinones v. State*, 766 So. 2d 1165, 1172 n.8 (Fla. 3d DCA 2000) ("The overwhelming authority in the nation concludes that an attorney may not accept evidence of a crime unless he or she makes the same available to the prosecutor or the investigating law enforcement agency.") and *Anderson v. State*, 297 So. 2d 871, 875 (Fla. 2d DCA 1974) (lawyer acted properly by surrendering evidence of a crime to police, and state cannot disclose circumstances in court).

Even if there is no duty under substantive law to disclose or return the documents, the inquiring attorney still has ethical obligations. The inquiring attorney owes the client the duty of confidentiality under Rule 4-1.6. Under this rule, a lawyer may not voluntarily reveal information relating to the representation of a client without the client's consent. Therefore, information which the inquiring attorney learns through the representation of the client is confidential under Rule 4-1.6, and cannot be revealed without the client's consent. There are exceptions to the duty of confidentiality. However, none seem to be applicable under the facts

presented, as any criminal act that the client may have been involved in is a past act and disclosure would not prevent a future crime.

On the other hand, the inquiring attorney cannot assist the client in conduct that the inquiring attorney knows or reasonably should know is criminal or fraudulent under Rule 4-1.2(d). Additionally, the inquiring attorney cannot engage in conduct involving dishonesty or that is considered prejudicial to the administration of justice under Rules 4-8.4 (c) and (d) and cannot violate the ethics rules through the acts of another, including the client, under Rule 4-8.4(a). Furthermore, Rule 4-3.4(a) provides that a lawyer must not "unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act."

The inquiring attorney needs to discuss the situation, including the ethical dilemma presented due to the client's actions, with the client. If the client possibly committed a criminal act, it may be prudent to have the client obtain advice from a criminal defense attorney if the inquiring attorney does not practice criminal law. The inquiring attorney should advise the client that the inquiring attorney is subject to disqualification by the court as courts, exercising their supervisory power, may disqualify lawyers who receive or review materials from the other side that are improperly obtained. *See, e.g.*, *Maldonado v. New Jersey, Administrative Office of the Courts –Probation Division*, 225 F.R.D. 120 (D. N.J. 2004). The inquiring attorney should also advise the client that the client is also subject to sanction by the court for her conduct. *See Perna v. Electronic Data Systems, Corporation*, 916 F. Supp 388 (D. N.J. 1995).

Finally, the inquiring attorney must inform the client that the materials cannot be retained, reviewed or used without informing the opposing party that the inquiring attorney and client have the documents at issue. *See The Florida Bar v. Hmielewski*, 702 So. 2d 218 (Fla. 1997). If the client refuses to consent to disclosure, the inquiring attorney must withdraw from the representation. *See* Rule 4-1.16(a)(1).

FLORIDA BAR ETHICS OPINION
OPINION 06-2
September 15, 2006

Advisory ethics opinions are not binding.

A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata. A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information's receipt. The opinion is not intended to address metadata in the context of discovery documents.

RPC:	4-1.1, 4-1.2, 4-1.4, 4-1.6, 4-4.4(b)
Opinions:	93-3, New York Opinion 749, New York Opinion 782
Case:	*Williams v. Sprint/United Management Company,* 230 F.R.D. 640, 96 Fair Empl.Prac.Cas. (BNA) 1775 (2005)
Misc:	David Hricik and Robert B. Jueneman, "The Transmission and Receipt of Invisible Confidential Information," 15 *The Professional Lawyer* No. 1, p. 18 (Spring 2004), *The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age,* Appendix F (The Sedona Conference Working Group Series, Sept. 2005 Series), Michael Silver, "Microsoft Office metadata: What you don't see can hurt you" *Tech Republic Gartner 2001*, Brian D. Zall, "Metadata: Hidden Information in Microsoft Work Documents and its Ethical Implications," 33 *Colo. Lawyer* No.10, p. 53 (Oct. 2004)

The Board of Governors of The Florida Bar has directed the committee to issue an opinion to determine ethical duties when lawyers send and receive electronic documents in the course of representing their clients. These ethical responsibilities are now becoming issues in the practice of law where lawyers may be able to "mine" metadata from electronic documents. Lawyers may also receive electronic documents that reveal metadata without any effort on the part of the receiving attorney. Metadata is information about information and has been defined as "information describing the history, tracking, or management of an electronic document."[1] Metadata can contain information about the author of a document, and can show, among other things, the changes made to a document during its drafting, including what was deleted from or

[1] *The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age,* Appendix F (The Sedona Conference Working Group Series, Sept. 2005 Series), available at http://www.thesedonaconference.org. The Microsoft Word and Microsoft Office online sites also contain detailed information about metadata, showing examples of metadata that may be stored in Microsoft applications and explaining how to remove this information from a final document. Examples of metadata that may be hidden in Microsoft documents include the name of the author, the identification of the computer on which the document was typed, the names of previous document authors and revisions to the document, including prior versions of a final document.

added to the final version of the document, as well as comments of the various reviewers of the document. Metadata may thereby reveal confidential and privileged client information that the sender of the document or electronic communication does not wish to be revealed. [2]

This opinion does not address metadata in the context of documents that are subject to discovery under applicable rules of court or law. For example, the opinion does not address the role of the lawyer acting as a conduit to produce documents in response to a discovery request.

The Florida Rules of Professional Conduct require lawyers to protect information that relates to the representation of a client. Rule 4-1.6(a) provides as follows:

> **(a) Consent Required to Reveal Information.** A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.

The Comment to Rule 4-1.6 further provides:

> A fundamental principle in the client-lawyer relationship is that the lawyer maintain confidentiality of information relating to the representation. The client is thereby encouraged to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter.

In order to maintain confidentiality under Rule 4-1.6(a), Florida lawyers must take reasonable steps to protect confidential information in all types of documents and information that leave the lawyers' offices, including electronic documents and electronic communications with other lawyers and third parties.

Rule 4-4.4(b) addresses inadvertent disclosure of information and provides as follows:

> A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.

The comment to rule 4-4.4 provides additional guidance:

> Subdivision (b) recognizes that lawyers sometimes receive documents that were mistakenly sent or produced by opposing parties or their lawyers. If a lawyer knows or reasonably should know that such a document was sent inadvertently, then this rule requires the lawyer to promptly notify the sender in

[2] Further references regarding metadata and eliminating metadata from documents may be found on Microsoft's user support websites at http://support.microsoft.com/kb/290945 and http://support.microsoft.com/kb/q223790/. *See also*, Michael Silver, "Microsoft Office metadata: What you don't see can hurt you" *Tech Republic Gartner 2001* http://techrepublic.com.com/5100-1035_11-5034376.html. The court's discussion of metadata in *Williams v. Sprint/United Management Company,* 230 F.R.D. 640, 96 Fair Empl.Prac.Cas. (BNA) 1775 (2005) is also very helpful.

order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning the original document, is a matter of law beyond the scope of these rules, as is the question of whether the privileged status of a document has been waived. Similarly, this rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained by the sending person. For purposes of this rule, "document" includes e-mail or other electronic modes of transmission subject to being read or put into readable form.

Some lawyers may choose to return a document unread, for example, when the lawyer learns before receiving the document that it was inadvertently sent to the wrong address. Where a lawyer is not required by applicable law to do so, the decision to voluntarily return such a document is a matter of professional judgment ordinarily reserved to the lawyer. See rules 4-1.2 and 4-1.4.

The duties of a lawyer when sending an electronic document to another lawyer and when receiving an electronic document from another lawyer are as follows:

(1) It is the sending lawyer's obligation to take reasonable steps to safeguard the confidentiality of all communications sent by electronic means to other lawyers and third parties and to protect from other lawyers and third parties all confidential information, including information contained in metadata, that may be included in such electronic communications.

(2) It is the recipient lawyer's concomitant obligation, upon receiving an electronic communication or document from another lawyer, not to try to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient. Any such metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit. *See*, Ethics Opinion 93-3 and Rule 4-4.4(b), Florida Rules of Professional Conduct, effective May 22, 2006.[3]

(3) If the recipient lawyer inadvertently obtains information from metadata that the recipient knows or should know was not intended for the recipient, the lawyer must "promptly notify the sender." *Id.*

---

[3] The ethical implications of such hidden information in electronic documents have been discussed in legal journals and ethics opinions in other states, The New York Bar Association has issued Opinion 749 (2001), which concluded that attorneys may not ethically use computer software applications to surreptitiously "mine" documents or to trace e-mail. New York Ethics Opinion 782 (2004), further concluded that New York lawyers have a duty to use reasonable care when transmitting documents by e-mail to prevent the disclosure of metadata containing client confidences or secrets. Legal commentators have published articles about ethical issues involving metadata. David Hricik and Robert B. Jueneman, "The Transmission and Receipt of Invisible Confidential Information," 15 *The Professional Lawyer* No. 1, p. 18 (Spring 2004). *See also*, Brian D. Zall, "Metadata: Hidden Information in Microsoft Work Documents and its Ethical Implications," 33 *Colo. Lawyer* No.10, p. 53 (Oct. 2004).

The foregoing obligations may necessitate a lawyer's continuing training and education in the use of technology in transmitting and receiving electronic documents in order to protect client information under Rule 4-1.6(a). As set forth in the Comment to Rule 4-1.1, regarding competency:

> To maintain the requisite knowledge and skill [for competent representation], a lawyer should engage in continuing study and education.

FLORIDA BAR ETHICS OPINION
OPINION 21-2
March 23, 2021

Advisory ethics opinions are not binding.

A lawyer ethically may accept payments via a Web-based payment-processing service (such as Venmo or PayPal), including funds that are the property of a client or third person, as long as reasonable steps are taken to protect against inadvertent or unwanted disclosure of information regarding the transaction and to safeguard funds of clients and third persons that are entrusted to the lawyer.

RPC: 4-1.1, 4-1.6(a), 4-1.6(e), 4-1.15, 5-1.1(a), (g)

I. Introduction

The Florida Bar Ethics Department has received several inquiries whether lawyers may accept payment from clients via Web-based payment-processing services such as Venmo and PayPal. This also is an increasingly frequent question on the Bar's Ethics Hotline. Accordingly, the Professional Ethics Committee issues this formal advisory opinion to provide Florida Bar members with guidance on the topic.

Several Web-based, mobile, and digital payment-processing services and networks ("payment-processing services") facilitate payment between individuals, between businesses, or between an individual and a business. Some are specifically designed for lawyers and law firms (e.g., LawPay and LexCharge), while others are not (e.g., Venmo, PayPal, ApplePay, Circle, and Square). These services operate in different ways. Some move funds directly from the payor's bank account to the payee's bank account, some move funds from a payor's credit card to a payee's bank account, and some hold funds for a period of time before transferring the funds to the payee. Service fees differ for various transactions, depending on the service's terms of operation. Some offer more security and privacy than others.

The Committee sees no ethical prohibition per se to using these services, as long as the lawyer fulfills certain requirements. Those requirements differ depending on the purpose of the payment—i.e., whether the funds are the property of the lawyer (such as earned fees) or the property of a client or third person (such as advances for costs and fees and escrow deposits). The two principal ethical issues are (1) confidentiality and (2) safeguarding funds of clients and third persons that are entrusted to the lawyer.

II. Analysis

A. *Confidentiality*

1. *The Issue*

The use of payment-processing services creates privacy risk. This arises from the potential publication of transactions and user-related information, whether to a network of subscribers or to a population of users interacting with an application. For example, Venmo users, when making a

payment, are permitted to input a description of the transaction (e.g., "$200 for cleaning service"). Transactions then are published to the feed of each Venmo user who is a party to the transaction. Depending on the privacy settings of each party to the transaction, other users of the application may view that transaction and even comment on it.

For lawyers, accepting payment through a payment-processing service risks disclosure of information pertaining to the representation of a client in violation of Rule 4-1.6(a) of the Rules Regulating The Florida Bar. Rule 4-1.6(a) prohibits a lawyer from revealing information relating to representation of a client absent the client's informed consent. This prohibition is broader than the evidentiary attorney-client privilege invoked in judicial and other proceedings in which the lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The ethical obligation of confidentiality applies in situations other than those in which information is sought from the lawyer by compulsion of law and extends not only to information communicated between the client and the lawyer in confidence but also to all information relating to the representation, whatever its source. R. Regulating Fla. Bar 4-1.6 cmt. para. [4]. Likewise, a lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation. *Id.* R. 4-1.6(e); *see also id.* R. 4-1.6 cmt. paras. [24], [25]. The obligation of confidentiality also arises from a lawyer's ethical duty to provide the client with competent representation. *See id.* R. 4-1.1 cmt. para. [3]. This includes safeguarding information contained in electronic transmissions and communications. *Id.*

Rule 4-1.6(c)(1) permits a lawyer to reveal confidential information to the extent the lawyer reasonably believes necessary to serve the client's interests. Although receipt of payment in connection with legal services benefits the client, the disclosure of information about the payment to a community of users would not. Wide publication of a Venmo payment "for divorce representation" hardly would serve the client's interest.[1]

2. *Recommended and Required Actions*

Payment-processing services typically offer various privacy settings. Venmo, for example, enables users to adjust their privacy settings to control who sees particular transactions. The options are (1) "Public," meaning anyone on the Internet will be able to see it, (2) "Friends only," meaning the transaction will be shared only with the "friends" of the participants to the transaction, and (3) "Private," meaning it will appear only on the personal feeds of the user and the other participant to the transaction. Venmo has a default rule that honors the more restrictive privacy setting between two users: if either participant's account is set to Private, the transaction will appear only on the feeds of the participants to the transaction, regardless of the setting enabled by the other participant.[2]

---

[1] Revealing to a bank the limited information needed to make a deposit to the lawyer's account serves the client's interest. In addition, financial institutions are subject to federal and state laws regarding disclosure of financial information.

[2] *See* Venmo Help Center, "Payment Activity & Privacy" available at https://help.venmo.com/hc/en-us/articles/210413717-Payment-Activity-Privacy.

If, as with Venmo, the service being used permits the recipient to control the privacy setting, the lawyer must select the most secure setting to mitigate against unwanted disclosure of information relating to the representation.

Venmo is only one example of a payment-processing service. Each application has its unique privacy settings and potential risks. The lawyer should be aware that these options can and likely will change from time to time. Prior to using a payment-processing service, the lawyer must diligently research the service to ensure that the service maintains adequate encryption and other security features as are customary in the industry to protect the lawyer's and the client's financial information and to preserve the confidentiality of any transaction. The lawyer must make reasonable efforts to understand the manner and extent of any publication of transactions conducted on the platform and how to manage applicable settings to preempt and control unwanted disclosures. *See* R. Regulating Fla. Bar 4-1.6(e); *id.* R. 4-1.1 cmt. para. [3]. The lawyer must take reasonable steps to avoid disclosure by the lawyer as well as by the client, including advising clients of any steps that they should take to prevent unwanted disclosure of information. Although not ethically required, inserting such advice in the lawyer's retainer or engagement agreement or on each billing statement is wise. For example:

> As a convenience to our clients, we accept payment for our services via certain online payment-processing services. The use of these services carries potential privacy and confidentiality risks. Before using one of these services, you should review and elect the privacy setting that ensures that information relating to our representation of you is not inadvertently disclosed to the public at large.
>
> The foregoing is just an example. Variations to fit the circumstances may be appropriate.

These confidentiality obligations apply to any payment that relates to the lawyer's representation of a client, regardless of the purpose of the payment.

B. *Safeguarding Funds of Clients and Third Persons*

1. *The Issue*

A customer's account with most payment-processing services such as Venmo and PayPal does not qualify as the type of bank account in which the trust-accounting rules require the funds of clients or third persons in a lawyer's possession be held. Indeed, with limited exceptions, they are not bank accounts at all, rather they are virtual ledgers of funds trading hands, with entries made by the service in the customers' names.

Rule 5-1.1(a)(1) of the Rules Regulating The Florida Bar establishes the fundamental anti-commingling requirement that a lawyer hold in trust, separate from the lawyer's own funds, funds of clients or third persons that are in a lawyer's possession in connection with a representation ("entrusted funds"). It requires that all such funds, including advances for fees, costs, and expenses, "be kept in a separate federally insured bank, credit union, or savings and loan association account maintained in the state where the lawyer's office is situated or elsewhere with the consent of the client or third person and clearly labeled and designated as a trust account."

All nominal or short-term entrusted funds must be deposited in an IOTA account. R. Regulating Fla. Bar 5-1.1(g)(2).[3] The IOTA account must be with an "eligible institution," namely, "any bank or savings and loan association authorized by federal or state laws to do business in Florida and insured by the Federal Deposit Insurance Corporation, any state or federal credit union authorized by federal or state laws to do business in Florida and insured by the National Credit Union Share Insurance Fund, or any successor insurance entities or corporation(s) established by federal or state laws, or any open-end investment company registered with the Securities and Exchange Commission and authorized by federal or state laws to do business in Florida." *Id.* R. 5-1.1(g)(1)(D).

2. *Recommended and Required Actions*

The Committee concludes that it is permissible for a lawyer to accept entrusted funds via a payment-processing service. To avoid impermissible commingling, the lawyer must maintain separate accounts with the service, one for funds that are the property of the lawyer (such as earned fees), which normally would be deposited in the lawyer's operating account, and one for entrusted funds (such as advances for costs and fees and escrow deposits), which when in a lawyer's possession are required to be held in a separate trust account. The lawyer must identify the correct account for the client or third party making the payment.

Rule 5-1.1 applies to funds of clients and third persons that are "in a lawyer's possession" and requires that any such funds be "kept" in a particular type of account. It does not require that the funds be "immediately" or "directly" deposited into a qualifying account. A payee does not acquire possession—access to and control over—funds transmitted via a payment-processing service until the service makes those funds available in the payee's account. If the funds are the property of the lawyer, the lawyer may leave those funds in that account or transfer them to another account or payee at the lawyer's discretion. The lawyer, however, must transfer entrusted funds from the service account into an account at a qualifying banking or credit institution promptly upon their becoming available to the lawyer. By transferring entrusted funds from the service account into a qualified trust account promptly upon acquiring access to and control over those funds, the lawyer complies with the requirement that those funds be *kept* in a qualified account.

Many banks do not permit linking an IOTA account to an account with a payment-processing service such as Venmo or PayPal. In those situations, the lawyer should establish with the banking institution some type of suspense account to which the account established with the payment-processing service can be linked and into which the payments are transferred, then promptly swept into the lawyer's IOTA account.

Depending upon how quickly the funds are released or other factors, a payment-processing service may charge the payee a transaction fee. Unless the lawyer and the client otherwise agree, the

[3] "Nominal or short-term" describes funds of a client or third person that the lawyer has determined cannot earn income for the client or third person in excess of the costs to secure the income. R. Regulating Fla. Bar 5-1.1(g)(1)(A). That determination involves consideration of several factors, such as the amount of the funds and the period of time that the funds are expected to be held. *See id.* R. 5-1.1(g)(3); *see also id.* R. 5-1.1(g)(1)(C) (definition of "IOTA account").

lawyer must ensure that any such fee is paid by the lawyer and not from client trust funds. Likewise, the lawyer must ensure that any chargebacks are not deducted from trust funds and that the service will not freeze the account in the event of a payment dispute. As with the concern for confidentiality, a lawyer must make a reasonable investigation into a payment-processing service to determine whether the service employs reasonable measures to safeguard funds against loss or theft and has the willingness and resources to compensate for any loss.

III. Conclusion

In sum, the Committee concludes that a lawyer ethically may accept payments via a payment-processing service (such as Venmo or PayPal), including funds that are the property of a client or third person that must be held separately from the lawyer's own funds, under the following conditions:

1. The lawyer must take reasonable steps to prevent the inadvertent or unwanted disclosure of information regarding the transaction to parties other than the lawyer and the client or third person making the payment.

2. If the funds are the property of a client or third person (such as advances for costs and fees and escrow deposits), the lawyer must direct the payor to an account with the service that is used only to receive such funds and must arrange for the prompt transfer of those funds to the lawyer's trust account at an eligible banking or credit institution, whether through a direct link to the trust account if available, through a suspense account with the banking or credit institution at which the lawyer's trust account is maintained and from which the funds automatically and promptly are swept into the lawyer's trust account, or through another substantially similar arrangement.

3. Unless the lawyer and client otherwise agree, the lawyer must ensure that any transaction fee charged to the recipient is paid by the lawyer and not from client trust funds. Likewise, the lawyer must ensure that any chargebacks are not deducted from trust funds and that the service will not freeze the account in the event of a payment dispute.

The Rules of Professional Conduct are "rules of reason" and "should be interpreted with reference to the purposes of legal representation and of the law itself." R. Regulating Fla. Bar ch. 4, pmbl. ("Scope"). When reasonable to do so, the rules should be interpreted to permit lawyers and clients to conduct business in a manner that society has deemed commercially reasonable while still protecting clients' interests. Permitting lawyers to accept payments via payment-processing services under the conditions expressed in this opinion satisfies those objectives.[4]

Note: The discussion about specific applications in this opinion is based on the technology as it exists when this opinion is authored and does not purport to address all such available technology. Web-based applications and technology are constantly changing and evolving. A

[4] The quoted language comes from the Preamble to the Rules of Professional Conduct, which are found in Chapter 4 of the Rules Regulating The Florida Bar. Rule 5-1.1 is part of the Rules Regulating Trust Accounts, which are found in Chapter 5 of the Rules Regulating The Florida Bar). Chapter 5 is incorporated into Chapter 4 by Rule 4-1.15.

lawyer must make reasonable efforts to become familiar with and stay abreast of the characteristics unique to any application or service that the lawyer is using.

December 22, 2021 **TECHREPORT 2021**

2021 Cybersecurity

David G. Ries

The threats to the security of data in computers, networks, and cloud services used by attorneys and law firms appear to be at an all-time high. And they continue to grow! ABA Formal Opinion 483, discussed below, starts with the following observation: "...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." The same is likely the case for law firms.

The ABA's *2021 Legal Technology Survey Report* explores security threats 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 safeguards covered in the questions in the survey and their use is generally increasing over time. However, it also shows that many law firms report that they are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions.

Significantly, 25% of respondents overall reported this year that their firms had experienced a data breach *at some time*.

Cybersecurity is addressed most directly in the "Technology Basics & Security" volume of the *2021 Survey*. This Cybersecurity *TechReport* reviews responses to the security questions and discusses them in light of both attorneys' duty to safeguard information and what many view as standard cybersecurity practices. It breaks down the information by firm size and compares it to prior years. 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

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and also often have contractual and regulatory duties to protect confidential information. These duties present a challenge to attorneys using technology because most are not technologists and often lack training and experience in security.

Several ethics rules in the ABA Model Rules have particular application to safeguarding client information, including competence (Model Rule 1.1), communication (Model Rule 1.4), confidentiality of information (Model Rule 1.6), and supervision (Model Rules 5.1, 5.2, and 5.3).

Together, these rules require attorneys, when using technology, to 1) employ competent and reasonable measures to safeguard the confidentiality of information relating to clients, 2) communicate with clients about the attorneys' use of technology and obtain informed consent from clients when appropriate, and 3) to supervise subordinate attorneys, law firm staff, and service providers to make sure that they comply with these duties.

Some ABA and state ethics opinions, for over a decade, have addressed these duties. There are three current relevant ABA formal ethics opinions, including ABA Formal Opinion 477R, "Securing Communication of Protected Client Information" (May 2017), ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 2018), and ABA Formal Opinion 498, "Virtual Practice" (February 2021).

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.

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." Law firms are covered by this resolution.

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 security incidents and data breaches. Cybersecurity programs should cover all of these functions.

An important initial step in establishing an information security program is assigning 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 appropriate (and affordable) only for larger law firms, every firm should have someone who is responsible for coordinating security. The larger the firm, the more it is necessary to have a full-time security officer or multiple persons who, together, are able to dedicate an appropriate part of their time and effort to security. The *2021 Survey* asks who has primary responsibility for security in respondents'

firms. As expected, responses vary by firm size. The respondents reported that they have primary responsibility in solo firms (80%), with external consultants/experts, IT staff, and a chief information officer having primary responsibility increasing with the size of firms. A chief security officer has primary responsibility in some large firms, 13% of firms with 100-499 attorneys, and 16% of firms with 500+. A small percentage (.9%) report that nobody has primary responsibility for security.

The *2021 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 *2021 Survey*, 53% of respondents report that their firms have a policy to manage the retention of information/data held by the firm, 60% report a policy on email use, 56% for internet use, 57% for computer acceptable use, 56% for remote access, 48% for social media, 32% personal technology use/BYOD, and 44% for employee privacy. The numbers have generally increased over the years and generally increase with firm size.

Two responses that raise a concern are those that report having no policies (17% overall) and those reporting that they don't know about security policies (8%). There is a clear trend by firm size in the responses of having no policies, with policies increasing with firm size. 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 a cybersecurity program. Overall, 36% report having an incident response plan. The percentage of respondents reporting that they have incident response plans varies with firm size, ranging from 12% for solos and 21% for firms with 2-9 attorneys to approximately 80% for firms with 100+ attorneys. 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 whom 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 if their law firm has any policies.

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

Recognizing the Risk

Cybersecurity starts with an inventory and risk assessment to determine what needs to be protected and the threats that an attorney or law firm 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. The next factors in the risk analysis cover appropriate safeguards. Comment [18] to ABA 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).

The *2021 Survey* includes information about the available safeguards that various attorneys and firms are using.

As noted above, about 25% 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 29% last year, 26% in 2019, 23% in 2018, and 22% in 2017. The number of attorneys reporting a breach at some time has generally increased over the years. The drop this year (29% last year to 25%) may not be meaningful because it asks about breaches ever.

This year, the reported percentage of firms experiencing a breach ranged from 17% of solos and firms with 2-9 attorneys, about 35% for firms with 10-49, 46% with 50-99, and about 35% with 100+. 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 firms' responses on breaches because the percentage of those reporting that they don't know about breaches (27% overall) directly goes up with firm size—reaching 58% in firms with 100+. 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 (48%) 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. A 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 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 *2021 Survey* shows a very low incidence of this result for firms that experienced a breach; about 7% overall. While the percentages are low, any exposure of client data can be a major issue for a law firm and its clients.

The information on breaches with exposure of client data is incomplete because 6% overall report that they don't know about the consequences. Unauthorized access to non-client sensitive data is 4% overall.

The other reported consequences of data breaches are significant. Downtime/loss of billable hours was reported by 36% of respondents; consulting fees for repair were reported by 31%, destruction or loss of files by 13%, and replacement of hardware/software reported by 18% (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 64% overall.

About 24% overall responded that they notified a client or clients of the breach. Formal opinion 483 addresses the duty to notify clients under Model Rule 1.4. The percentage reporting notice to clients ranges from 33% for solos and firms with 2-9, 9% for firms with 10-49, none for firms with 50-99, 18% for firms with 100-499, and 70% for firms with 500+.

Overall, 14% of respondents that experienced a breach reported that they gave notice to law enforcement, ranging from 13% for solos to 70% for firms with 500+.

The *2021 Survey* also inquired whether respondents ever experienced an infection with viruses/spyware/malware. Overall, 29% reported infections, 39% reported none, and 32% reported that they don't know. 61% reported no

significant business disruption or loss.

Basic security measures like using up-to-date security software, using current versions of operating systems and software, promptly applying patches to the operating system and all application software, employing effective backup, and training of attorneys and staff, can help to protect against these kinds of threats.

Security Assessments and Client Requirements

Clients are increasingly focusing on the cybersecurity 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 27% of law firms overall reporting that they had a full assessment. Affirmative responses generally increase with the size of the firm.

Overall, 30% of respondents report that they have received a client security requirements document or guidelines, with affirmative responses generally increasing by firm size. There is a growing recognition in the cybersecurity security

profession of the importance of securing data that business partners and service providers, including law firms, can access, process, and store.

Cyber Insurance

As the headlines continue to be filled with reports of data breaches, 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 has been increasing— 42% overall, this year. 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 cybersecurity 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 comprehensive cybersecurity programs. Some firms use them as guidelines for their security programs, while a smaller group of firms have

obtained formal security certification under a standard. The *2021 Survey* asks whether respondents' firms have received a security certification. Overall, only 12% report that they have received a certification, with a low for firms with 2-9 (4%) and a high for firms with 500+ (28%).

Basic Security Tools

The *2021 Survey* asks about various security tools that are available to responding attorneys. Many 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 81% 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 software-based firewalls (75%), anti-spyware (75%), mandatory passwords (70%), antivirus for desktops/laptops as well as for e-mail (both about 70%) and networks (66%), and hardware firewalls (57%). The 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. There is a general low incidence of "don't know" responses for these tools, about 9% overall. Attorneys and law firms that are not using all of these tools should review the ones that they are not using, with qualified assistance if needed.

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. This part of the *2021 Survey* includes a general question about mandatory passwords, without specifying the access for which they are required. Overall, 70% of respondents report using mandatory passwords. They are required by 50% of solos, 73 % of firms of 2-10 attorneys, and about 80% or higher for larger firms. About 11% of firms overall report using biometric login. Some form of strong authentication should be required for access to computers and networks for all attorneys and all law firms.

Multifactor authentication is being increasingly used to provide a stronger form of authentication. There are three authentication factors: something the user knows (like a password), something the user has (like a security token or a security app on a smartphone), and something the user is (like a fingerprint or face scan). Multifactor authentication uses two or three of these factors. If a password is compromised or brute-forced, an attacker cannot get access without the second factor. The Cybersecurity and Infrastructure Security Agency (CISA) recently added failure

to use multifactor authentication for remote access and administrator access to its list of Bad Practices. (The other Bad Practices on the current list are using unsupported [end-of-life] software and using known/default passwords.)

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 *2021 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 the use of the correct password or other access control. Respondents report an overall use of full drive encryption of only 20%, ranging from 17% for solos to about 63% for firms of 500+, 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—50% overall, ranging from 30% for solos to 81% in firms of 500+. This question is general and is not broken down by servers, desktops, laptops, smartphones, etc.

Verizon's 2014 *Data Breach Investigation Report* (over seven years ago) concluded 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?

Intrusion Detection Prevention software (IDS) and Intrusion Prevention software (IPS) detect or block some attacks on networks or computers. Respondents reported an overall use of about 53% for each of them. Use increases by the size of firm, with solos reporting 18% for IDS and 22% for IPS and firms with 500+ reporting about 53% for both.

Additional security tools covered in this volume of the Survey, with reported overall usage include pop-up blockers (67%), network antivirus (62%), hardware firewalls (52%), file access restrictions (46%), and employee monitoring (20%).

Disaster Recovery/Business Continuity

Threats to the availability of data can range from the 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 and insecure remote access. It encrypts a user's or network's data and demands a ransom (to be paid by Bitcoin) for the

release of the decryption key. Effective backup, which is isolated from production networks, can sometimes provide timely recovery from this aspect of ransomware. Unfortunately, attackers often exfiltrate (steal) data before encrypting it and demand an extortion payment or they will sell or publish the data.

Overall, 15% of respondents report that their firm had experienced a natural or man-made disaster, like a fire or flood. The highest incidence, about 26%, was in firms of 50-99. The lowest reported incidence was for solos at 8%, with the rest being between these numbers. Disasters of this kind can put a firm out of business—temporarily or permanently. These positive responses 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 48% 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 24% of solos to 80% of firms with 500+ attorneys. As with comprehensive security programs, all law firms should have a disaster recovery/business continuity plan, appropriately scaled to its size.

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 3% report that they don't back up their computer files. 33% of respondents report that they don't know about backup. The

most frequently reported form of backup is external hard drives (28%), followed by online backup and offsite backup (each 25%), network-attached storage (12%), USB (7%), cloud (5%) (appears to overlap with online), RAID (4%), CDs (5%), tape (3%), DVDs (2%), and other (2%). The most common methods for solos and small firms are external hard drives and online. A majority of attorneys in firms of 50+ attorneys report that they don't know.

The *2021 Survey* responses show that 41% of respondents use constant live backup, 26% back up once a day, 10% more than once a day, 9% weekly, 3% monthly, and 1% quarterly. 10% report that they don't know, with unknowns increasing with firm size.

With the increasing risks of ransomware, hardware failures, disasters, and other incidents reported in the *2021 Survey*, attorneys and law firms should consider reevaluating the methods and frequency of backups, if they have not recently done so. Cybersecurity professionals recommend maintaining multiple backups, including offline and offsite backups.

Conclusion

The *2021 Survey* provides a good overview, with supporting details, of what attorneys and law firms are doing to protect information relating to clients. Like the last several years, it generally shows increasing attention to security and increasing use of the covered safeguards, but also

demonstrates that there is still 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 should 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.

ENTITY:

LEGAL TECHNOLOGY RESOURCE CENTER, LAW PRACTICE DIVISION

TOPIC:

PRACTICE MANAGEMENT, TECHNOLOGY, CYBERSECURITY

Authors

> "By the time law firms notice the breach, it may have already suffered financial loss, and, consequently, media attention and reputational harm. A robust cybersecurity compliance program would help the firm secure the data against improper access and use. In other words, maintaining strong cybersecurity policies within your firm is key to mitigating liability exposure." – Dr. Nick Oberheiden, Founding Attorney of Oberheiden P.C.

2020 Statistics on Cybersecurity and Law Firms

The American Bar Association's Legal Technology Resource Center compiles an annual report on cybersecurity for law firms that discusses the adoption of compliance programs, types of cyber risks, and injuries caused from cybersecurity breaches. The number of law firms reporting a security breach increased from 26% in 2019 to 29% in 2020. Some of these results may have been impacted by COVID-19 since many law firms moved operations online—thus necessitating virtual work environments and online communications.

Security breaches analyzed in the ABA's report were broad and included stolen computers, exploiting vulnerabilities in websites, and hacking. Law firms experiencing viruses, spyware, or other infection within their company must expend significant amounts of time, energy, and money in correcting the issue.

A recent example, in 2019, a senior director of corporate law and lawyer at Apple was charged and indicted on insider trading charges. The indictment alleged that the lawyer traded confidential information during a blackout period where no stock can be bought or sold.

Legal Obligations for Law Firms: Statutes on Cybersecurity

There is no federal law regulating a law firm's cybersecurity practices and policies. However, federal law does regulate specific industry practices. For instance, if a law firm has a client within the healthcare, accounting, or financial industry sectors, additional federal obligations may apply.

Clients in the financial industry sector may require that their law firms maintain extra security protection due to the sensitive nature of financial data. The same applies for healthcare companies who store confidential health records of the public. Clients that specialize in accounting practices must comply with the Sarbanes–Oxley Act of 2002, which could impose additional obligations on the law firms representing those clients.

The failure of the law firms to properly safeguard client data in these circumstances could lead to federal investigations, lawsuits, loss of future clients, fines and penalties, and significant reputational harm.

In addition to industry standards encompassed by federal law, each state has its own laws regulating data protection. Law firms in California must be mindful of the California Consumer Privacy Act, while law firms in New York must take account of the regulations of the New York State Department of Financial Services as well as the Stop Hacks and Improve Electronic Data Security ("SHEILD") Act.

Law firms may also find it beneficial to adhere to cybersecurity guidelines. The National Institute of Standards and Technology ("NIST") is a non-regulatory agency within the Department of Commerce that provides guidelines for cybersecurity regulations for the federal government. NIST standards are voluntary but compliance with NIST's Cybersecurity Framework is good practice for law firms and provides good evidence that the law firm took sufficient measures to comply with cybersecurity-related laws and industry practices.

Ethical Obligations for Law Firms: Protecting Client Data and Maintaining

Confidentiality

State boards are responsible for regulating the conduct of lawyers and law firms. To do this, state boards often issue ethical opinions to guide them on appropriate cybersecurity practices within their law firms. Specifically, U.S. law firms have to adhere to the ABA's Model Rules of Professional Conduct.

Model Rule of Professional Conduct 1.4 requires attorneys to make sure that clients are "reasonably informed about the status of the matter" and to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

Further, Model Rule of Professional Conduct 1.6 states that lawyers must make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 8 to Model Rule 1 explains that, in order to maintain the required knowledge and skill, lawyers should stay abreast of all changes "including the benefits and risks associated with relevant technology."

ABA Formal Opinion 483 on "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" provides that lawyers have a duty to make "reasonable efforts to avoid data loss or to detect cyber-intrusion" and that an ethical violation may occur if the lawyer does not undertake these steps.

Thus, because law firms often do business with colleagues, opposing counsel, federal agencies, and clients via electronic communications, they have an obligation to ensure that all data is properly stored, secured, and safeguarded

Internal Obligations for Law Firms: Strengthening Cybersecurity from the Inside

Law firms are finding it beneficial to adopt or strengthen their internal practices to strengthen overall cybersecurity. Examples of supplements to a law firm's cybersecurity include the following:

- Cyber insurance
- Cloud backup
- Encryption software
- Reboot and backup policies
- Strong firewalls
- Risk assessment and internal controls
- Robust cybersecurity compliance program
- Crisis response plan for cyberattacks
- Reliable antivirus software
- Strong password combination
- Strict controls over personnel access to sensitive information
- Using only secured Wi-Fi

Conclusion

Cybersecurity breaches of a law firm's sensitive or confidential data can lead to lawsuits, investigations, fines and penalties, and unwanted media attention. It can not only hurt the law firm's ability to attract clients in the future but also the reputation of the individual attorneys.

Attorneys implicated in data breaches and other cybersecurity risks undermine the attorney's duties of competency and confidentiality.

To prevent such disastrous consequences that will follow from these breaches, many law firms follow strict legal, ethical, and internal obligations regarding strong cybersecurity practices. Obligations such as compliance with industry standards and state laws; ABA ethical rules, and internal best practices within the law firm enable the law firm to mitigate cybersecurity risk.

National Law Review, Volume XI, Number 189
Source URL: https://www.natlawreview.com/article/5-cybersecurity-risks-and-3-obligations-law-firms