Staff Memorandum

HOUSE OF DELEGATES
Agenda Item #9

REQUESTED ACTION: Approval of the report and recommendations of the Committee on Technology and the Legal Profession.

Attached is a report from the Committee on Technology and the Legal Profession recommending that NYSBA support amendment of the mandatory continuing legal education rule be amended to require one credit in cybersecurity. The credit would be included within the "ethics and professionalism" category and would not add to the minimum 24-hour biennial rule for experienced attorneys or the 32-hour biennial requirement for new attorneys. The amendment would be effective for four years and revisited after that time.

The committee notes that New York ethics rules require lawyers to keep up with technology and to exercise reasonable care in preventing disclosure of confidential information. Accordingly, educating attorneys regarding cybersecurity has taken on increased importance. Both Florida and North Carolina have added a technology requirement to their CLE requirements. Rather than recommend a general technology requirement, the committee believes cybersecurity protection is a pressing issue for lawyers and should be emphasized through a one-credit requirement.

This report was published in the Reports Community February 2020. The Local and State Government Law Section has indicated that it opposes the proposal, and the Trusts and Estates Law Section indicates that it supports.

The report will be presented at the June 13 meeting by committee co-chair Mark A. Berman.

REPORT RECOMMENDING THAT THE ATTORNEY CONTINUING LEGAL EDUCATION BIENNIAL REQUIREMENT BE MODIFIED TO REQUIRE THAT THE ETHICS AND PROFESSIONALISM REQUIREMENT INCLUDE FOR FOUR YEARS ONE CREDIT ON CYBERSECURITY

COMMITTEE ON TECHNOLOGY AND THE LEGAL PROFESSION

OF THE

NEW YORK STATE BAR ASSOCIATION

January 27, 2020

Opinions expressed are those of the Committee preparing the Report and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

COMMITTEE ON TECHNOLOGY AND THE LEGAL PROFESSION

CO-CHAIRS

Mark A. Berman

Ganfer Shore Leeds & Zauderer LLP

Gail L. Gottehrer

Law Office of Gail Gottehrer LLC

COMMITTEE MEMBERS

Seth Agata
Alison Arden Besunder
Shoshanah V. Bewlay
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
Maura R. Grossman
Ronald J. Hedges
Shawndra Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Sanford Strenger
Ronald P. Younkins

EXECUTIVE SUMMARY

The Committee on Technology and the Legal Profession (the "Committee") of the New York State Bar Association ("*NYSBA*") proposes to the Executive Committee of *NYSBA* that it recommend that the biennial, twenty-four hour credit requirement for attorney continuing legal education requirement ("CLE") contained in the CLE Board Rules and Regulations be modified to require one credit on the topic of cybersecurity. The credit would be considered under "*Ethics and Professionalism*" and it would be included within the existing biennial "*Ethics and Professionalism*" requirement. The one credit would not add to the already-required thirty-two (32) credit hours for new attorneys or the twenty-four (24) hours for more experienced attorneys. The requirement would exist for four years and would be revisited thereafter and potentially be extended depending on the state of the legal profession at the time regarding cybersecurity, including the "hacking" of law firm electronically stored information.

INTRODUCTION

NYSBA has a long history of being on the cutting edge of CLE requirements for lawyers. *NYSBA* considers technological competence in the practice of law to be essential to respond effectively to the needs of our changing society and a CLE requirement designed to educate lawyers on how to protect confidential and proprietary client and law firm electronic assets relates directly to legal competency.

Mandatory CLE was initially conceived, supported and implemented as a way to enhance both lawyer competence and public trust in the profession. The ABA's 1992 MacCrate Report, entitled "*Law Schools and the Profession: Narrowing the Gap*," provided a platform for states considering whether to mandate CLE requirements and identified four basic values of professional responsibility. As described by one commentator in 1998, the four values are: "1) providing

competent representation; 2) striving to promote justice, fairness and morality; 3) striving to improve the profession; and 4) professional self-development." Including a mandatory cybersecurity component will help advance those values by providing attorneys with ongoing education in this critical area and increasing public trust that their confidential and proprietary information will be secure when in the possession of attorneys.

THE LANDSCAPE OF HACKING IN THE LEGAL PROFESSION

The *New York Law Journal* ("*NYLJ*") reported in an October 2019 article, entitled "Eight NY Law Firms Reported Data Breaches as Problems Multiply Nationwide," that the number of law firm data breaches in New York State doubled in 2018 and that "[d]espite a number of high-profile breaches putting firms on notice of cyber risks in recent years, there are indications that law firm breaches are occurring more frequently, not less." The article also reported that some cybersecurity lawyers and consultants said the numbers "likely represent a tiny fraction of the breaches affecting the legal industry. Law firms, like other privately held businesses, don't often publicize when their data is breached, and many may not report it to state officials, depending on the law." The *NYLJ* also reported in an October article entitled, How Vendor Breaches Are Putting Law Firms at Risk, that "[e]xternal breaches, including phishing and hacking as well as vendor incidents, were the most commonly identified source of data exposure events reports by law firms."

Also, in an October 2019 article, entitled "As Hackers Get Smarter, Can Law Firms Keep Up?," the *NYLJ* reported that "large and small law firms can do much better in preventing and reacting to data breaches" and "cautioned that the legal sector may risk falling behind other industries." The *NYLJ* noted that "[w]hile hackers are getting smarter, it's also the case that some law firms aren't keeping up with security guidelines developed inside the industry and in other

professional fields, according to legal industry surveys and interviews with security consultants and law firm leaders." The article quoted Austin Berglas, former head of the FBI's cyber branch in New York, as stating that "he would rate law firm cybersecurity as 'middle of the road' now, as firms juggle the competing interests of access and security."

The article then quoted Logicforce, an IT law firm consulting company that had surveyed midsize law firms, which noted that the legal industry "remains very vulnerable to cyberattacks." The article noted that, according to the survey, "fewer firms in 2019 compared with last year's survey reported implementing prevention techniques such as multifactor authentication and data loss prevention technology, which can scan and block the transmission of personally identifiable information." Critically, the *NYLJ* article made clear that "[e]thics laws require lawyers to keep pace with technology to protect client information. Still, some observers point to a slow pace of budding ethics rules on cybersecurity questions."

NEW YORK'S ETHICAL FRAMEWORK

NYSBA Committee on Professional Ethics Op. 950 provides:

> A fundamental principle in the client-lawyer relationship "is that, in the absence of the client's informed consent or except as permitted or required by the Rules of Professional Conduct (the "Rules"), the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source." Rule 1.6, Cmt. [2]. The attorney not only has an obligation to refrain from revealing such information, but also must *exercise reasonable care* to prevent its disclosure or use by "the lawyer's employees, associates, and others whose services are utilized by the lawyer." (emphasis added).

NYSBA Committee on Professional Ethics Op. 1019 provides that the duty of "reasonable care"

> does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality

> include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

In fact, NYSBA Committee on Professional Ethics Op. 842 provides that a lawyer must take reasonable care to *affirmatively* protect a client's confidential information. It further provides that:

> [c]yber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent)
>
> In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information.

New York ethics opinion make clear that lawyers have an affirmative duty to protect confidential and proprietary client and law firm information and to stay current on cybersecurity threats, including the risk of being electronically compromised and what anticipatory or counter-measures should be reasonably implemented in order to appropriately safeguard client and law firm confidential and proprietary information.

The education of lawyers on the issue of cybersecurity has become even more imperative now that New York has enacted the "*Stop Hacks and Improve Electronic Data Security*" or "*SHIELD Act*," which applies to all law firms, even to solo practitioners and small firms. The *SHIELD Act* creates, for the first time, substantive security requirements for persons or businesses that hold the "private information" of New York residents, and it: (1) expands the types of data that may trigger data breach notification to include user names or e-mail addresses, and account, credit or debit card numbers; (2) broadens the definition of a breach to include unauthorized "access" (in addition to unauthorized "acquisition"); and (3) creates a new reasonable security requirement for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of" private information of New York residents. Safeguards may include designating employees to coordinate a security program, conducting risk assessments and employee training on security practices and procedures, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and securely disposing of private information within a reasonable time.

The *SHIELD Act*, as it applies to solo practitioners and small law firms, requires those persons and entities to ensure that there "are reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

OTHER STATES NOW MANDATE TECHNOLOGY CLE CREDIT

The Florida Supreme Court approved a rule requiring Florida lawyers to take a minimum of three hours of technology-related CLE courses during a three-year cycle. In addition to adding the three-hour requirement, the Court amended a comment to its rule on lawyer competence to

state that lawyers could retain nonlawyer advisers with "established technological competence in the relevant field." The Court added that competent representation may also involve cybersecurity and safeguarding confidential information. The Court also noted that "in order to maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education, including an understanding of the risks and benefits associated with the use of technology."

The North Carolina Supreme Court also recently approved a mandatory CLE rule. It provides that:

> "Technology training" shall mean a program, or a segment of a program, devoted to education on information technology (IT) or cybersecurity (see N.C. Gen. Stat. §143B-1320(a)(11), or successor statutory provision, for a definition of "information technology"), including education on an information technology product, device, platform, application, or other tool, process, or methodology. To be eligible for CLE accreditation as a technology training program, the program must satisfy the accreditation standards in Rule .1519 of this subchapter: specifically, the primary objective of the program must be to increase the participant's professional competence and proficiency as a lawyer. Such programs include, but are not limited to, education on the following: a) an IT tool, process, or methodology designed to perform tasks that are specific or uniquely suited to the practice of law; b) using a generic IT tool process or methodology to increase the efficiency of performing tasks necessary to the practice of law; c) the investigation, collection, and introduction of social media evidence; d) e-discovery; e) electronic filing of legal documents; f) digital forensics for legal investigation or litigation; and g) practice management software. See Rule 1602 of this subchapter for additional information on accreditation of technology training programs.

THE COMMITTEE'S APPROACH

The Committee considered recommending that a general technology component be added as a required subject under New York Bar's CLE requirement, as did Florida and North Carolina; however, the Committee agreed that such a general requirement may result in attorneys not actually focusing on what the Committee believes to be one of the most pressing and urgent issues facing our legal profession: cybersecurity protection of confidential and proprietary client and law firm electronic information and assets, which includes protecting client and law firm monies

maintained in escrow and operating accounts, all of which are subject to phishing, scams, impersonation, fraud and other wrongful artifices. The Committee believes that requiring attorneys to take one credit in cybersecurity will sensitize and educate lawyers on how to secure confidential and proprietary client and law firm electronic information, and when and how to notify clients and/or law enforcement, as appropriate, in the event of a cyber incident.

Lastly, notwithstanding reporting by the press on data breaches and, more importantly on law firm breaches, the Committee has been surprised by the relative lack of attendance at *NYSBA* CLEs on cybersecurity, whether in person or over webinars.

CONCLUSION

Accordingly, we request that the Executive Committee of the NYSBA support this important initiative by voting in support of the Committee's recommendation.

To: Committee on Technology and the Legal Profession
From: Trusts & Estates Law Section, CLE Committee
Date: May 8, 2020
Re: Proposed Modification of MCLE Requirements

The Committee on Technology and the Legal Profession of the New York State Bar Association has proposed a modification of the New York State CLE Board Regulations & Guidelines (*see* "Report Recommending that the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require that the Ethics and Professionals Requirement Include for Four Years One Credit on Cybersecurity," January 27, 2020). The proposed modification is that, for a period of four years — two biennial registration periods — one of the credit-hours of continuing legal education already mandated in the area of ethics and professionalism (*see* 22 NYCRR §1500.12 [a] [1] and 22 NYCRR §1500.22 [a]) be devoted to cybersecurity. At the end of the four-year period, the Committee on Technology and the Legal Profession would evaluate whether to extend the requirement. We recommend that the proposal be approved. Safeguarding client information in electronic form is a timely and important ethics issue for attorneys practicing in New York State.

COMMENTS ON THE REPORT OF THE COMMITTEE ON TECHNOLOGY AND THE LEGAL PROFESSION BY THE LOCAL AND STATE GOVERNMENT LAW SECTION

These comments are respectfully submitted by the Local and State Government Law Section (the "Section") on the report of the Committee on Technology and the Legal Profession (the "Committee") entitled "Report Recommending that the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require that the Ethics and Professionalism Requirement Include for Four Years One Credit on Cybersecurity" dated January 27, 2020.

While the Section agrees with the Committee that cybersecurity for law firms is of critical importance, and agrees that this subject should be offered as an option to fulfill the required continuing legal education ("CLE") ethics credits, we disagree with the recommendation that it be mandatory that one credit of the four required CLE ethics credits be on this topic for the following reasons:

1. It has not been demonstrated that cybersecurity is a topic over which most attorneys have control. Many attorneys, particularly those employed by larger law firms and government entities, have little, if any, ability to control or influence their employer's cybersecurity policies and do not typically handle escrow funds. Similarly, they do not control the choice of vendors to be used by their employers, or those vendors' cybersecurity choices or protections. While the Section recognizes that phishing emails and hacking attempts may be sent to any attorney, and that attorneys should be educated about how to avoid such attempts, this topic does not require an hour of CLE for every attorney for every biennial reporting period. The first line of defense is the email software utilized by the attorney's employer, whether firm or governmental entity, and the majority of attorneys have no control over those choices.

2. Enacting this requirement effectively limits the amount of CLE programming that the Section can provide on ethical subjects specific to Section members during Section meetings. One of the Section's goals has been to provide, during its in-person Fall and Annual Meetings, sufficient CLE opportunities for the members to satisfy their CLE requirements. Given the finite time available for programming during Section meetings, particularly the annual meeting in New York City, the imposition of this requirement will mean, as a practical matter, that a portion of the time otherwise devoted to Section-specific ethical education will be replaced with this more general CLE instruction in order to fulfil the requirement, thereby diluting the member benefit of providing Section-specific information. While it is true that the Section could offer additional substantive and ethical programming via webinars throughout the year to make up for this change, it is not as optimal as engaging in the ethical discussions of municipal law subjects that typically occur at the in-person meetings.

3. As a corollary to the second point, the assertion may be made that the Section (or another entity) could provide the cybersecurity requirement via webinar or at a separate meeting. While technically correct, this also raises concerns. For example,

Section attorneys are not typically cybersecurity experts, and the Section likely would need to locate outside sources to provide this education to their members. Some governmental entities typically provide their attorneys with in-house CLE. The City of New York is an example. If this requirement is imposed, the City will be burdened with either developing new courses to satisfy this requirement or obtaining the materials from outside sources, neither of which is optimal because, as noted in item 1 above, few of their employees would have any decision-making authority concerning cyber-security.

In sum, the goal of sensitizing attorneys to cybersecurity issues is laudable. However, it can be achieved by methods other than making training a mandatory hour of education for every attorney.

Tannenbaum Helpern
Syracuse & Hirschtritt LLP

900 Third Avenue New York, NY 10022-4775
Tel: (212) 508-6700 | Fax: (212) 371-1084
www.thsh.com | @THSHLAW

Vincent J. Syracuse
Direct Dial: (212) 508-6722
Fax: (212) 371-1084.
E-mail: Syracuse@thsh.com

June 5, 2020

Mark A. Berman, Esq.
Ganfer Shore Leeds Zauderer LLP
360 Lexington Avenue
New York, New York 10017

Re: Report Recommending that the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require that the Ethics and Professionalism Requirement Include for Four Years One Credit on Cybersecurity (the "Cybersecurity Report")

Dear Mark:

I am a member of the NYSBA Committees on Attorney Professionalism and Continuing Legal Education and a former Chair of the Commercial & Federal Litigation Section. I have also authored over 75 Attorney Professionalism Forums in the NYSBA Journal since January 2012.

I write to support the adoption of the Cybersecurity Report by the House of Delegates at tomorrow's meeting. I endorse the proposal that for a period of four years one of the credit-hours of continuing legal education already mandated in the area of ethics and professionalism (*see* 22 NYCRR §1500.12 [a] [1] and 22 NYCRR §1500.22 [a]) be devoted to cybersecurity with an evaluation whether to extend the requirement to take place at the end of the four years. As emphasized in our June/July Forum, which discusses the ethical and professional challenges that we have all been facing practicing law during the pandemic, the protection of client information from cybersecurity threats is an ethical issue of paramount importance to all attorneys practicing in New York State and should be make a part of the continuing legal education ethics requirement.

Sincerely,

s/Vincent J. Syracuse

Vincent J. Sryacuse

[1127761-1]

NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, New York 12207 PH 518.463.3200 www.nysba.org

To: Mark Berman & the Committee on Technology and the Legal Profession

From: Young Lawyers Section

The Young Lawyers Section supports the proposed modification to the MCLE requirements contained in the Report your Committee prepared. We agree that it is critical for all lawyers in New York State to fully understand and appreciate the necessity of cybersecurity. Including cybersecurity as part of the MCLE requirements would ensure that law firms are better equipped to practice law in 2020 and beyond. Especially as we work from home, relying on digital technology to engage with our clients, our colleagues, the courts and others, it is imperative that we practice securely.

Reprinted with permission from: New York State Bar Association *Journal*, June/July 2020, Vol. 92, No. 5, published by the New York State Bar Association, One Elk Street, Albany, NY 12207.

The Attorney Professionalism Committee invites our readers to send in comments or alternate views to the responses printed below, as well as additional hypothetical fact patterns or scenarios to be considered for future columns. **Send your comments or questions to: NYSBA, One Elk Street, Albany, NY 12207, Attn: Attorney Professionalism Forum, or by email to journal@nysba.org.**

This column is made possible through the efforts of the NYSBA's Committee on Attorney Professionalism. Fact patterns, names, characters and locations presented in this column are fictitious, and any resemblance to actual events or to actual persons, living or dead, is entirely coincidental. These columns are intended to stimulate thought and discussion on the subject of attorney professionalism. The views expressed are those of the authors, and not those of the Attorney Professionalism Committee or the NYSBA. They are not official opinions on ethical or professional matters, nor should they be cited as such.

TO THE FORUM:

I am the managing partner of a general practice law firm of approximately 40 lawyers and 20 staff members. In response to the ongoing pandemic, all firm employees are required to work from home. While the safety of the firm's employees is always a top priority, our management team has concerns about how our employees remain in compliance with their ethical obligations during this time. Specifically, with many of our attorneys working in close quarters to other family members, how can they best ensure they are safeguarding client's confidentiality?

Additionally, our firm has implemented a number of practices to facilitate a seamless transition when working from home. For example, we provide secure remote access protected with two-factor authentication for access to our work applications. We also provide a firm-hosted cloud-based file sharing service so that our employees can transfer multiple and high-volume files to clients as well as one another throughout the workday. Are there any specific ethical obligations we should be aware of with respect to the technology and working from home? How can our firm ensure that we are using technology safely, effectively and in compliance with our ethical obligations?

Separately and surprisingly, we have reached out to adversaries requesting extensions of deadlines, and one adversary in particular was obstinate refusing to give us an extension, despite the fact that my client was one of the many individuals who had become sick because of the pandemic, forcing us to make an application to the court. Is our adversary's conduct ethical? What principles of ethics should we adhere to when dealing with unreasonable adversaries?

Lastly, given that face-to-face communications are severely limited and individual accessibility is uncertain, what are our ethical obligations with respect to the supervision of subordinate attorneys and staff?

Sincerely,
Patty Partner

DEAR PATTY:

The global pandemic has undoubtedly forced us to steer a course through uncharted professional territory. It has created many professional and ethical challenges as lawyers have been compelled to practice law primarily in a remote work environment.

One of the most fundamental challenges that lawyers face when working from a remote location is the necessity to protect client confidences. As discussed in prior Forums, RPC 1.6 governs a lawyer's duty of confidentiality, and this duty applies in all settings and at all times.

When working at home, it is easy to adopt casual practices. Attorneys should be wary of falling into that trap. Working remotely often creates unique circumstances of having to work in close proximity to other family members. As a result, attorneys must take extra precautions to safeguard client confidences. For example, your "remote office" should be as autonomous as possible. It is best practice to avoid working in commonly used areas of your home such as the kitchen table or the living room.

However, we understand that this might not be feasible in every situation, especially for attorneys with younger children engaging in remote learning. If your circumstances do not permit you to create a designated and private workspace within your home, you should endeavor to set clear boundaries with children, partners and other members of your household as to how they should treat your workspace and work files. You also may want to consider investing in a locked filing cabinet to store sensitive information. If you do not have locked storage, we suggest that you store your work-related materials somewhere only you can access them. Attorneys should also consider practical efforts, such as not letting children or significant others access work devices for personal use and setting up a private, password-protected, Wi-Fi network specifically for your professional work. At a minimum, your work devices (laptops, tablets, phones) should always be password-protected with strong and unique passwords.

We also suggest that you do your best to become "tech-savvy" or competent in the technology you will need when working remotely. The NYSBA Committee on Professional Ethics (the "Committee") has opined that an attorney should only use technology that he or she is competent to use. See NYSBA Comm. on Prof'l Ethics, Op. 1025 (2014). Accordingly, a law firm should take appropriate steps to ensure that its attorneys are familiar with the firm's operating systems and computer programs and the firm's policies concerning the use of those systems/programs before transitioning to a fully remote work environment.

But, that is only half the battle. Attorneys also should be cognizant of the heightened risk of cybersecurity threats when working remotely. Comment [8] to RPC 1.1 states: "to maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information." As addressed in a prior Forum, attorneys and law firms have an ethical obligation to institute and maintain sound cybersecurity protocol, and to ensure that third-party vendors do the same. See Vincent J. Syracuse, Maryann C. Stallone, Richard W. Trotter & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., June 2017, Vol. 89, No. 5.

Phishing scams are an example of a common cybersecurity threat to law firms. These scams include fraudulent emails that appear to be sent from a genuine source, such as a colleague, family member or personal banking institution, for the purpose of obtaining personal information, such as passwords and banking details, and defrauding attorneys or their firms. For this reason, attorneys should be extra vigilant when reviewing emails and downloading files. It is always a best practice to double check the email address of the sender and confirm the email is legitimate, as many hackers will create fake email accounts with only slight variations to that of the individual the hacker is purporting to impersonate. Attorneys also should avoid downloading files or clicking on links from an email that they are not expecting, and immediately bring emails that appear to be suspicious to the attention of the firm's IT department for further investigation.

Furthermore, we recommend that attorneys access their firm networks remotely through a Virtual Private Network (VPN), an encrypted connection over the internet from a device to a network. The encrypted connection

helps ensure that sensitive data is safely transmitted over the internet. Firms should always keep their VPNs current and deploy all patches with updated security configurations. Moreover, it is critical to maintain proper multi-factor authentication for all VPN access to networks.

Cybersecurity threats also arise with the use of cloud-based file-sharing services to send and receive confidential client documents. A 2014 report by the Department of Homeland Security recognized that "online tools that help millions of Americans work from home may be exposing both workers and businesses to cybersecurity risks." Michael Roppolo, Work-from-home remote access software vulnerable to hackers: Report, CBS News (July 31, 2014).

In two ethics opinions issued in 2014, the Committee concluded that giving lawyers remote access to client files was not unethical, as long as the technology used provides reasonable protection to confidential client information, or the law firm informs the client of the risks and obtains informed consent from the client to proceed. See NYSBA Comm. on Prof'l Ethics, Op. 1019 (2014) and NYSBA Comm. on Prof'l Ethics, Op. 1020 (2014). In Opinion 1019, the Committee noted that "because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients." Id. However, Comment [17] to RPC 1.6 instructs us that "[t]he key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure." RPC 1.6, Comment [17].

To meet the reasonable care standard set forth in RPC 1.6, attorneys should consult with their firm's IT department or service provider to investigate whether their firm's file-sharing services implement reasonable security measures to protect client confidence. Where possible, the firm should implement two-factor authentication to access its work applications and software. If after speaking with your IT provider/personnel you continue to have doubts as to security, you should obtain the client's consent before sharing any files or documents. The failure to employ basic data-security measures can have severe consequences, including civil liability for professional malpractice.

A security measure that law firms should consider implementing to protect client confidences is the encryption of files and emails sent both inside and outside the firm. Encryption is the process of converting digital information into a code, to prevent unauthorized access by outside parties

Additional best practices in addressing cybersecurity risks include: (1) understanding and using reasonable security measures, such as secure internet access methods; when accessing files remotely, attorneys should avoid logging on to unsecured Wi-Fi networks or "hotspots," which can expose both the attorney and the firm's files to malware – software designed by hackers that can infiltrate remote desktops and whose capabilities include logging keystrokes, uploading discovered data, updating malware and executing further malware; (2) training non-lawyer support staff in the handling of confidential client information and to report suspicious activity; (3) clearly and conspicuously labelling confidential client information as "privileged and confidential"; (4) conducting due diligence on third-party vendors providing digital storage and communication technology; (5) creating and implementing a data breach incident response plan; and (6) assessing the need for cyber insurance for data breaches. See ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 477 (May 2017).

Using secure internet access is of critical importance to avoid a man-in-the-middle attack, or "MITM" attack, which occurs when the communication between two systems is intercepted by a third party, i.e., a Man-in-the-Middle. This can happen in any form of online communication, such as email, web-browsing, and even social media. The MITM can use a public Wi-Fi connection to gain access to your browser, or even compromise your entire device. Once the MITN gains access to your device they have the ability to steal your credentials, transfer data files, install malware, or even spy on the user. To avoid the potentially significant and disastrous effects of a MITM attack, you should work off a secure Wi-Fi network and avoid using "hotspots."

Additionally, when using video-conferencing platforms such as Zoom, make sure that your meetings are password-protected to avoid a type of cyberattack called "Zoom-bombing," where strangers hijack a private Zoom teleconferencing chat and draw offensive imagery onscreen, such as pornographic images, personal information of the individuals in the chat, and even taunting them with hate speech and threats.

Turning to the part of your question regarding the civility (or lack thereof) of your adversary, the pandemic is certainly no excuse for bad behavior. As discussed in a recent Forum, RPC 3.4 governs "fairness to opposing party and counsel" and provides that when dealing with an opposing party and the opposing party's counsel, an attorney must act with fairness and candor. See RPC 3.4; see also Vincent J. Syracuse, Maryann C. Stallone, Carl F. Regelmann & Alyssa C. Goldrich, Attorney Professionalism Forum, N.Y. St. B.J., April 2020, Vol. 92, No. 3. The commentary to Rule 1.2 further provides that in

accomplishing the client's objectives, the lawyer should not be offensive, discourteous, inconsiderate or dilatory. RPC 1.2 Comment [16]. And, while the RPC does not specifically address an attorney adversary's obligations under Rule 3.4 or 1.2 in the wake of a global pandemic, it is axiomatic that lawyers should be particularly sensitive to reasonable requests for extensions under such circumstances.

While your adversary's refusal to grant you a reasonable extension is not a per se violation of the RPC or a basis for a report to the Disciplinary Committee, such conduct may violate the New York State Standards of Civility (the "Standards"), particularly if this is the first time you are asking for an extension on the motion. See 22 N.Y.C.R.R. § 1200, App. A. As discussed in a prior Forum, the Standards of Civility were adopted as a guide for the legal profession, including lawyers, judges and court personnel, and outline basic principles of behavior to which lawyers should aspire. See Vincent J. Syracuse, Maryann C. Stallone & Hannah Furst, Attorney Professionalism Forum, N.Y. St. B.J., March/April 2016, Vol. 88, No. 3.

The language of the Standards of Civility is clear – in the absence of a court order, a lawyer should agree to reasonable requests for extensions of time when the legitimate interests of the client will not be adversely affected. See 22 N.Y.C.R.R. § 1200, App. A. An adversary who refuses to provide a reasonable extension during the global pandemic in order to gain some tactical advantage is not just exhibiting bad form, but is creating a negative reputation and relationship with their adversary that may ultimately adversely affect their position in the litigation. By way of example, an uncooperative attorney is unlikely to get a professional courtesy in the future. Moreover, judges and juries generally do not look kindly upon attorneys that do not extend professional courtesies. In the ordinary course, reasonable requests for extensions of time should be handled by the attorneys in the case, not by the courts.

The flip side to this scenario, which is also likely to occur, is attorneys using the pandemic as an excuse for their dilatory tactics to delay the case and frustrate your client's ability to recover. As is the case with many ethical rules, the deciding factor in whether to grant or deny a request for an extension is the reasonableness of the request.

Separately, your obligations with respect to the supervision of subordinate attorneys remain unchanged. RPC 5.1 sets forth the responsibilities of law firms, partners, and managers over other lawyers. Lawyers serving in a managerial or supervisory role are required to make reasonable efforts to ensure that all attorneys comply with their ethical obligations. This duty becomes even more important in a time of disaster or emergency. See RPC 5.1. Specifically, RPC 5.1(b) requires lawyers with management or direct supervisory authority over other lawyers in the firm to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the RPC such as identifying dates by which actions must be taken in pending matters and ensuring that inexperienced lawyers are appropriately supervised. See RPC 5.1, Comment [2].

There are no bright line rules governing supervision. Comment [3] to RPC 5.1 tells us that each law firm should carefully consider the structure and nature of its practice when adopting policies governing the supervision of subordinate attorneys. See RPC 5.1, Comment [3]. For example, if the firm is relatively small and consists of mostly experienced lawyers, informal supervision and periodic review of compliance with the required policies will ordinarily suffice. Conversely, if the firm is much larger, and employs numerous junior attorneys, more elaborate measures may be necessary to place the firm in compliance with RPC 5.1. Id.

The degree of supervision required also varies on a case-by-case basis and is generally judged by what is reasonable under the circumstances. Factors that should be considered include: (i) the experience of the person whose work is being supervised, (ii) the amount of work involved in a particular matter, and (iii) the likelihood that ethical problems might arise while working on the matter. See id.

Generally speaking, it is best practice for supervising attorneys to remain apprised of subordinate attorneys' workload, implement a system for review of the subordinate attorney's work product and ensure that the subordinate attorney understands that system. In our experience, requiring subordinate attorneys to submit weekly status reports detailing the matters they are working on is a good first step to guarantee that no matter falls through the cracks.

Supervising attorneys also should establish an open line of communication with subordinate attorneys. In today's age, there are many mediums that allow for regular communication in this remote work environment, including video conferencing (via Zoom or Skype), telephone calls, email and even text messages. Therefore, in addition to communicating via email, a supervising attorney should schedule regular calls (via Zoom, Skype or telephone) with subordinate attorneys to check on their progress and review and discuss their work product and workload. How often you communicate with the individuals under your supervision will depend on the complexity of the matter and issues, and the upcoming deadlines in those matters. This too is a matter of the lawyer's reasonable judgment and care.

Notably, RPC 5.1(d) articulates a general principle of personal responsibility for acts of other lawyers in the law firm and imposes such responsibility on a lawyer who orders, directs or ratifies wrongful conduct and on lawyers who are partners or who have comparable managerial authority in a law firm who know or reasonably should know of the conduct. See RPC 5.1(d). Thus, lawyers acting in a supervisory or managerial role should be aware that their failure to exercise diligence in reviewing the work of subordinate attorneys may result in personal liability under RPC 5.1(d).

Whether you are working in the office or remotely, attorneys should always use their best efforts so that client communication and diligent representation continues uninterrupted. One of our prior Forums referred attorneys to RPC 1.4, which governs an attorney's obligations with respect to communicating with clients. RPC 1.4 states that attorneys are ethically obligated to promptly comply with reasonable requests for information from clients. RPC 1.4(a)(4); see Vincent J. Syracuse, Maryann C. Stallone & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., July/August 2016, Vol. 88, No. 6. To avoid noncompliance with RPC 1.4 while working remotely, attorneys should inform clients of the best way to reach them. If, for example, an attorney is able to forward calls from the office line to a personal cell phone, the attorney can tell clients that they may still use the office number. If attorneys do not have this ability, they need to advise their clients what alternate number they can be reached at (whether a cell phone number or home landline). In addition, attorneys should regularly check their office voicemail and email and avoid large gaps in response time.

Finally, attorneys must continue to maintain their professionalism and decorum despite working from the comfort of their homes. We have previously talked about the importance of dressing appropriately when appearing in front of a tribunal; proper dress is part of basic professionalism and a sign of respect. See Vincent J. Syracuse & Matthew R. Maron, Attorney Professionalism Forum, N.Y. St. B.J., May 204, Vol. 86, No. 4. That standard still applies when participating in a virtual court conference, as well as video arbitrations and mediations. Judge Dennis Bailey of Broward County Florida recently expressed his dismay that attorneys appeared inappropriately on camera for virtual court hearings: "It is remarkable how many attorneys appear inappropriately on camera," Bailey said. "We've seen many lawyers in casual shirts and blouses, with no concern for ill-grooming, in bedrooms with the master bed in the background, etc. One male lawyer appeared shirtless and one female attorney appeared still in bed, still under the covers. And putting on a beach cover-up won't cover up that you're poolside in a bathing suit. So, please, if you don't mind, let's treat court hearings as court hearings, whether Zooming or not." Debra Cassens Weiss, Lawyers are dressing way too casual during Zoom court hearings, judge says, ABA Journal (Apr. 15, 2020), https://www.abajournal.com/news/article/lawyers-are-dressing-way-too-casual-during-zoom-hearings-judge-says.

As always, the devil is in the details. What is deemed appropriate can be subjective, and there may not always be agreement on what should be worn when in a virtual court or ADR proceeding. Certainly, going shirtless, wearing a bathing suit or video conferencing from your bed is never appropriate. You should use common sense, and when in doubt, it is best to err on the side of caution and overdress to avoid facing the risk of having your choice of clothing overshadow the needs of your client or what you might be saying.

Sincerely,
The Forum by
Vincent J. Syracuse, Esq.
(syracuse@thsh.com)
Maryann C. Stallone, Esq.
(stallone@thsh.com) and
Alyssa C. Goldrich, Esq.
(goldrich@thsh.com)
Tannenbaum Helpern Syracuse & Hirschtritt LLP

QUESTION FOR THE NEXT ATTORNEY PROFESSIONALISM FORUM:

DEAR FORUM:

I am an attorney in private practice focusing on personal injury law here in New York. I also do a bit of matrimonial law. My clients come from underserved communities, and many face extreme financial hardships. I've always known that Rule 1.8(e) prohibits giving financial assistance to clients in connection with a pending litigation and, as much as I have wanted to, I never gave anyone a dime. Rather, over the years, I developed a nice Rolodex with contacts at public service associations to refer these clients to so they could get their needs met. But with all this Covid-19 stuff going on it has gotten way worse and so many have now found themselves without a paycheck and are simply unable to meet their day-to-day needs. The public service organizations have been inundated, and my clients are unable to get desperately needed help. I was recently approached by a client, a young parent of two preschool-aged children, who is unable to buy groceries. And while I know that I probably shouldn't have, I figured that it would be okay to give him a few bucks for a couple of bags of groceries. He's a good kid and I know the money is going to his children. I am concerned I may have done something wrong but it really was so little to me and so much to him. What should I have done?

Sincerely,
Justa Bene Mensch