Emerging Ethical Issues and Hot Topics

Julian C. Zebot
Maslon LLP
Minneapolis, MN[1]

A host of emerging issues resulting from legal or technological developments with respect to the practice of law have created increased uncertainty as to lawyers' professional responsibilities and ethical duties. While the landscape has changed, the Model Rules of Professional Conduct—subject to certain exceptions—have not. This presentation will focus on the way the constantly changing and evolving practice of law intersects with our ethical duties as attorneys, focusing on remote/virtual work environment, the use of generative AI, and emerging know-your-client obligations.

I. The Starting Point - Model Rules of Professional Conduct

A. Competence - MRPC 1.1

MRPC 1.1 provides that, "a lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

Comment 8 to MRPC 1.1 makes clear that to maintain the requisite knowledge and skill to be competent, a lawyer should keep abreast not only of changes in the law in that lawyer's area of practice, but also should stay educated on, "the benefits and risks associated with relevant technology."[2]

B. Diligence – MRPC 1.3

A lawyer must act with reasonable diligence and promptness in representing a client.[3] This duty can come under strain when working remotely for extended periods of time and will place on the lawyer a greater focus on the ability to access files (especially if stored physically at an office and not digitally), regularly checking mail sent to the office, especially important client related communications and having systems in place for continuing to communicate with lawyers notwithstanding physical isolation from other. The lawyer must seek to proceed with the representation of a client to the best of the lawyer's abilities under the changing circumstances of remote work. Further, if a lawyer will be on extended leave because of illness or other reason, this rule requires that the lawyer should have processes in place for continuing representation of the client by other lawyers - whether within that lawyer's firm or others if the lawyer is a solo practitioner.

---

[1] Mr. Zebot is a Partner at Maslon LLP in Minneapolis, MN, where he chairs the firm's Trust and Estate Litigation practice group and serves as its ethics counsel. A special thank you goes to Mel Justak of Reed Smith LLP for his contributions to a prior set of presentation materials on which these materials are in part based.
[2] MRPC 1.1, Comment 8.
[3] MRPC 1.3.

Citing Comment 1 of MRPC 1.3, ABA Formal Opinion 498 (hereinafter "Opinion 498"), , emphasizes that "lawyers must also pursue a matter on behalf of a client despite opposition, obstruction, or personal inconvenience."[4]

C. Communication – MRPC 1.4

A lawyer has a duty to keep a client reasonably and promptly informed. Specifically, the lawyer must keep the client reasonably informed about the status of the matter, and promptly comply with reasonable requests for information.[5] Opinion 498 goes further to provide that a lawyer shall consult with the client about the means by which the client's objective are to be accomplished, keep the client reasonably informed about the status of the matter, and promptly comply with reasonable requests for information.[6]

As will be explored in greater detail below, attorneys may have a duty to communicate with their clients regarding their use of generative AI on client-related matters. In the remote work context, the lawyer must regularly check voicemail and email to ensure no communications are missed, and firms must have a system to regularly handle physical mail.

D. Confidentiality – MRPC 1.6

MRPC 1.6 imposes a duty of confidentiality on lawyers to all clients. Subject to certain enumerated exceptions, this rule broadly prohibits a lawyer from revealing "information relating to the representation of a client." MPRC 1.6(c), additionally requires that lawyers make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Paragraphs 18 and 19 of the comments to MPRC 1.6 address the application of the rules with respect to the use of modern technology. Specifically, paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. While "the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure"[7] the question remains what are "reasonable efforts"? Further, when transmitting confidential communications, "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[8] Again, while this comment is helpful in framing the issue, the question becomes what would be considered "reasonable precautions"?

---

[4] Opinion 498, Section II, A., 1.
[5] MRPC 1.4(3) and (4).
[6] Note 4, supra.
[7] MRPC 1.6, Comment 18.
[8] MRPC 1.6, Comment 19.

Opinion 498 provides a series of factors a lawyer could consider when determining the reasonableness of the lawyer's efforts including, but not limited to:

(a) The sensitivity of the information;

(b) The likelihood of disclosure if additional safeguards are not employed;

(c) The cost of employing additional safeguards;

(d) The difficulty of implementing the safeguards;

(e) 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).[9]

Keep in mind that a client or local law may require the lawyer to implement special security measures not required by the above rules.

E. Supervision – MRPC 5.1 and 5.3

Pursuant to MRPC 5.1(a), a partner or other lawyer in a law firm with "comparable managerial authority" is obligated to "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." Additionally, "[a] lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.[10] A similar duty extends to the lawyer's supervision of non-attorney staff as well.[11] In circumstances where the supervising attorney becomes aware of an ethical violation, he or she may have a duty to undertake corrective action. Notably, where a law firm or its partner fail to exercise adequate supervision, these rules serve to impose vicarious responsibility for the supervised attorney's or staff member's own breaches of the rules.

II. Navigating Virtual Practice (Ethically)

Opinion 498 provides best practices for the remote/virtual work environment to help ensure that the lawyer's technology, other assistance, and work environment are consistent with the lawyer's ethical obligations. In order to effectively and ethically navigate virtual practice, lawyers must manage technological, as well as human, considerations, each of which will be addressed in turn below.

A. Managing the Technology

When operating in the remote/virtual work environment, lawyers should ensure that their hardware and software systems offer sufficient protection of confidential data. Among other best practices, lawyers should be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption. Lawyers should also periodically assess whether

[9] Opinion 498, Section II, A., 2.
[10] MRPC 5.1(b).
[11] MPRC 5.3.

their existing systems are adequate to protect confidential information. Lawyers should use virtual private networks (VPNs) and secure Wi-Fi routers where possible.[12]

PRACTICE POINTER: *While it should go without saying, lawyers should not use the public hotspot at the library or the neighborhood coffee shop's Wi-Fi to conduct client business.*

Additional safeguards may not be as apparent. For example, be sure to save data only on secure office networks and not on personal devices. Also, while many clients increasingly appear to prefer text message communications, it is still preferable to communicate over your office email network (assuming it employs reasonable encryption) rather than through unencrypted texts.

Lawyers practicing virtually must ensure that they have reliable access to client contact information and records. If access to such files is provided through a cloud service, the lawyer should choose (1) a reputable company, and (2) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer. Lawyers must ensure that data is regularly backed up and that a secure backup is available in case of data loss. Lawyers should have a data breach policy and plan to communicate losses or breaches to impacted clients.

PRACTICE POINTER: *If your office network has the ability to remotely access client files via an encrypted network, be sure to use that system exclusively for accessing client's data. If using a third party cloud storage vendor, be sure it offers proper security protocols to protect a client's confidential information. Pay special attention as well to the vendor's data breach notification policy so clients can be notified after the lawyer receives notice of a data breach.*

When accessing your office's network—regardless of whether you are working in the office or a remote location—be sure to lock your computer when stepping away so unauthorized parties are not able to access sensitive client information.

Lawyers should take reasonable precautions to ensure that their use of a virtual meeting platform is consistent with their ethical obligations. Lawyers should also consider upgrading their platform to the highest tiers of security. All recordings and transcripts should be secured. If ever recording a client video conference and not otherwise required by local law or local ethics opinions, it is inadvisable to record such meetings without first having the client give informed consent. Lawyers should also take steps to ensure that only authorized parties are able to hear the video conference in progress.[13]

PRACTICE POINTER: *When using Zoom or other videoconferencing services, be sure to not make the meetings public (e.g., login information provided on social media), require a password for admittance that is randomly generated for that particular meeting and provide the login credentials directly to the participants only. Be sure that only the host can manage screen sharing features and admit attendees. If taking the call at home or in a location that is not*

[12] Opinion 498, Section II., B., 1.
[13] Opinion 498, Section II., B., 3.

totally private, try to isolate in a separate room and use headphones when on the call to lessen the risk of others outside of the zone of privilege inadvertently hearing the conversations.[14]

Lawyers' virtual document and data exchange platforms should ensure that documents and data are being appropriately archived for later retrieval and that the service or platform is and remains secure.[15]

PRACTICE POINTER: *If your office network allows for a secure document-sharing site where clients can send and receive documents over an encrypted pathway, try to use that exclusively. If sending .pdf documents to clients over email, password protect each file and provide the password to the client via other means and not in the same email containing the attachments. If using outside vendors to share documents, be sure the lawyer understands the level of encryption used and security protocols for storing the documents and in the event of a data breach.*

Be mindful of the requirements that clients may have for secure communications including sensitive data (e.g., secure emails utilized by financial institutions).

Lawyers should disable the listening capability of devices or services such as smart speakers, virtual assistants, and other listening-enabled devices while communicating about client matters unless the device or service is assisting the lawyer's law practice. Otherwise, the lawyer is exposing client information to unnecessary and unauthorized third parties and increasing the risk of hacking.[16]

PRACTICE POINTER: *Turn off Alexa and Siri in the office and be careful of discussing client matters at home or in non-office locations where these devices may be engaged.*

B. Managing the People

While the duty to supervise under Rules 5.1 and 5.3 may be familiar to most lawyers within the office setting, it may be less so in the virtual or remote work environment, where there may be greater practical difficulties in "keeping tabs" on subordinate attorneys and staff.

By way of Opinion 498, the ABA attempted to provide some guidance applicable to the virtual work environment setting. To be clear, lawyers must still provide their assistants with "appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."[17] Moreover, a lawyer must "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."[18]

---

[14] Opinion 498, Note 21 (discussing Pennsylvania best practices).
[15] Opinion 498, Section II., B., 4.
[16] Opinion 498, Section II., B. 5.
[17] MPRC 5.3, Comment 2.
[18] MPRC 1.6, Comment 18.

> Lawyers with managerial authority have ethical obligations to establish policies and procedures to ensure compliance with the ethics rules, and supervisory lawyers have a duty to make reasonable efforts to ensure that subordinate lawyers and nonlawyer assistants comply with the applicable Rules of Professional Conduct.[19]

The ABA has been clear in noting that "[p]racticing virtually does not change or diminish this obligation."[20] Comment [3] to Model Rule 5.3 underscores the fact that when services outside of the firm are utilized, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The duty to supervise does not end at the office door.

The ABA recommends that the virtual lawyer adopt policies and practices "to ensure that all members of the firm and any internal or external assistants operate in accordance with the lawyer's ethical obligations of supervision."[21] So what can you do to ensure that this, in fact, happens?

PRACTICE POINTER: *When dealing with subordinate attorneys or assistants, be sure to maintain open lines of communication and regular interaction with associates, paralegals, and legal assistants—making sure that proper avenues are created in case questions from subordinates arise. If your firm has a bring-your-own-device policy, make sure subordinates are trained in proper data security and that your firm has a system in place to protect client information if devices are lost, stolen, or otherwise inaccessible. Finally, ensure your subordinates are working in spaces where confidential client information is not visible to others. This includes ensuring that videoconferences involving client-related information are held in areas where the audio or video is not perceivable to others.*

When dealing with outside vendors, it is critical that the supervising lawyer ensure that all of these individuals or services comply with the lawyer's obligation of confidentiality and other ethical duties. When appropriate, lawyers should consider use of a confidentiality or business associate agreement, and should ensure that all client-related information is secured, indexed, and readily retrievable.

What are some best practices for exercising effective supervisory oversight in the virtual or remote work environment?

- Schedule regular check-ins—working from home should not mean "out of sight, out of mind."

- Have a virtual "open door" policy—invite calls or questions from subordinates when in legitimate doubt as to what to do. Do not encourage suffering in silence.

- Emphasize (and utilize) mentoring relationships—this is particularly important for more junior associates.

[19] Opinion 498, at 3 (citing MPRC 5.1 & 5.3).
[20] *Id*.
[21] Opinion 498, at 6.

- Where you see gaps, speak up—if you see areas of concern, speak with your firm and your teams to discuss how those issues can be resolved.

The duty to supervise extends to attorney wellness. In recent years, greater attention has been paid to the connection between attorney wellness, client service, and professional ethics—including, most significantly, the impact of wellness on the duties of competence (Model Rule 1.1) and diligence (Model Rule 1.3). Among other groups, the National Task Force on Lawyer Well-Being has studied these issues and attempted to identify and recommend best practices and solutions that can be adopted by lawyers and law firms to address them.

The numbers surrounding mental illness and substance abuse within the legal profession are truly staggering. According to several studies, as many as 1 in 4 attorneys either has a mental health or substance-abuse disorder or is at risk of developing one. Somewhat counterintuitively, younger attorneys (particularly those under the age of 30) have been shown to be even more likely to suffer from either depression or a substance-abuse disorder than older attorneys. Given this reality, the duty to supervise necessarily encompasses efforts to identify and support younger colleagues who need supportive assistance in dealing with, and proactively addressing, such issues.

So what can be done, particularly in the virtual work environment, to maintain a reasonably watchful eye on attorney wellness issues? Long term, cultural change is needed within most law firms to successfully address these issues. Law firm leaders and supervisors need to (1) identify stakeholders and their roles in bringing about cultural change; (2) diminish stigma associated with seeking help for mental health disorders; (3) emphasize within their organization that well-being is part of the duty of competence; (4) expand educational outreach on mental health and substance use disorders, as well as issues related to well-being; and (5) change the tone within their organization to make health and well-being a top priority for everyone.

In terms of day-to-day management of subordinate attorneys and staff, law firm leaders and supervisors need to be carefully attuned to behavioral changes in the attorneys or staff that they supervise, and they need to create some safe space in which the affected attorney can seek out assistance, rather than simply suffer in silence. In some cases, it may be as simple as asking your subordinate, "how are you <u>really</u> doing?"

As the Director of Minnesota's Office of Lawyers Professional Responsibility noted, "vicarious civil and criminal liability for the acts of others is beyond the scope of the ethics rules. . . . Nor are you strictly liable for the conduct of others."[22] Subject to that caveat, the Director noted:

> However, you can be professionally liable under these rules in basically three ways: (1) you are a covered attorney who did not have reasonable measures in place, or make reasonable efforts appropriate to your role, and misconduct occurred; (2) you order or, with knowledge of the conduct, ratify the misconduct; or (3) you are a covered attorney, you know of the misconduct at a time when consequences can be avoided or mitigated, and you fail to take remedial action.[23]

[22] Humiston, *Your ethical duty of supervision*, Bench & Bar of Minnesota (Dec. 2019).
[23] *Id.* (citing MPRC Rule 5.1, Comment 6; MPRC 5.1(c); MRPC 5.3(c)).

Director Humiston provides several examples where discipline was imposed for failure to adequately supervise:

i. Subordinate Forgery

In one instance, a solo attorney failed to put adequate measures in place to prohibit and detect the fact that her paralegal was forging her name on numerous pleadings and falsely notarizing affidavits of service in multiple cases; the attorney received a public reprimand.[24]

ii. Subordinate Embezzlement

In another case, an attorney failed to supervise or establish adequate measures to prevent his long-time office manager from stealing client and firm funds; the attorney received a lengthy suspension.[25]

III. Generative AI – Burying Your Head Is Not an Option

As noted above, lawyers have an ethical duty to keep abreast of changes in the law and its practice, including the benefits and risk associated with relevant technology." Some states have taken this rule a step further and advise that if a lawyer doesn't understand a certain technology, they should seek out a nonlawyer or someone with relevant expertise to help. Additionally, when using generative AI, lawyers must know enough about the AI technology to consider whether the tool is appropriate for the representation and be mindful of accuracy concerns. If a lawyer chooses to affirmatively incorporate generative AI into their practice, they have a duty to understand how it works. Even if they have no desire to be on the technological "bleeding edge," generative AI is rapidly being incorporated into practice-based technologies, so even the most reluctant luddite has a duty to stay on top of these developments.

Consistent with Rule 1.4, "[a] lawyer shall reasonably consult with the client about the means by which the client's objectives are to be accomplished." At a minimum, "this duty will require consultation prior to taking action." Likewise, Rule 1.6 precludes "a lawyer [from] reveal[ing] information relating to the representation of a client" absent the client's "informed consent" (or the existence of another exception to the general duty of confidentiality).

These rules inevitably raise practical questions with respect to how, and to what extent, lawyers are expected to discuss the use of generative AI with their clients. For example, how would a client expect their lawyer to use generative AI (if at all)? Should the lawyer disclose their (potential) use of generative AI in their engagement letter? If they do insert such verbiage into their engagement letter, does that constitute sufficient consultation? For what it is worth, ABA Formal Opinion 512 has questioned whether the addition of boilerplate language to an engagement letter is sufficient to obtain a client's "informed consent" to the use of generative AI during the course of the representation and the attendant risk that confidential information will be inadvertently disclosed by way of the technology's use.

[24] *Id.* (citing *In re Naros*, 928 N.W.2d 915 (Minn. 2019)).
[25] *Id.* (citing *In re Rosso*, 919 N.W.2d 477 (Minn. 2018)).

But, to be clear, just because you can, doesn't mean you should. Even with the client's "informed consent," lawyers should entertain second thoughts about providing generative AI tools with certain particularly sensitive types of client information, including the following:

- Personal identifying information
- Intellectual property
- Financial information
- Proprietary information
- Anything that should not be generally available to the public

Beyond the MRPC, there is an ever-increasing patchwork of state and federal privacy requirements governing the use of generative AI by lawyers. For example, certain states recognize additional financial or tax-information privileges or privacy rights that might preclude the use of generative AI. For example, tax preparers are required to comply with the IRC §7216, which imposes criminal penalties ($1,000 file and 1 year imprisonment/violation) for the reckless disclosure of any information furnished in connection with delivery of tax services or preparation of any tax return and expressly prohibits the preparer from disclosing a taxpayer's information without their explicit consent.

Additionally, following the *Mata* sanctions order, individual courts and judges, both state and federal, have increasingly begun to adopt either local rules or standing orders governing the use of generative AI work product in court filings, which often impose attorney certification requirements. For example, judges in the Northern District of Texas, the Eastern District of Pennsylvania, the Northern District of Illinois, and the United States Court of International Trade have embraced such requirements. Even in jurisdictions that have not yet done so, litigators should always carefully consider FRCP Rule 11's requirements when relying upon generative AI with respect to work product that will be filed under the lawyer's signature. Given the non-uniform nature of these court-imposed requirements, a lawyer should always satisfy themselves that their local jurisdiction does not impose a more set of stringent requirements regarding the use of generative AI than those imposed by the MRPC.

One final reason not to bury one's head is the duty to supervise. As a reminder, "[w]ith respect to a nonlawyer… [a managerial lawyer] shall make reasonable effort to ensure the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer." In short, you must supervise your young lawyers and staff (and your old ones too)—and, in order to do so, you must acquire a working understanding of generative AI tools, their risks, their benefits, and how they intersect with your ethical and legal obligations as a lawyer.

IV. Know-Your-Client Obligations – A Slow (But Inevitable?) Creep

Traditionally, lawyers have not been treated as "'gatekeepers' of corporate responsibility in the same fashion as public accounting firms."[26] That said, in recent years, there has been an increased legislative and regulatory push to require lawyers to abide by the same know-your-client ("KYC") and anti-money laundering ("AML") requirements that apply to other professional service providers.

For instance, the ENABLERS Act ("Establishing New Authorities for Businesses Laundering and Enabling Risks to Security Act") was introduced in October 2021 by a bipartisan lawmakers in response to the release of the Pandora Papers. Aimed at closing loopholes that allowed "enablers" to launder illicit funds in the United States, the ENABLERS Act would extend AML requirements to professional service providers, including accountants, lawyers, and third-party payment services. The House of Representatives passed a revised version of ENABLERS Act in July 2022, but the Senate ultimately voted against the act's inclusion in the defense budget.

Even absent new legislation, the Treasury Department had been, prior to the change in administration, working with Congress and banks to determine whether lawyers, accountants and other "gatekeeper professions" should fall under existing AML requirements, but no proposal appears imminent.[27] The prospects for new anti-AML regulation remain uncertain at the current time.

Nonetheless, the legal profession has attempted to stay a step ahead of such regulatory developments. In April 2020, ABA Formal Opinion 491 was issued. It addresses a lawyer's obligations Under Rule 1.2(d) to avoid counseling or assisting in a crime or fraud in non-litigation settings. Specifically, Opinion 491 attempts to clarify the intersection of Rules 1.2 and 1.16 where a lawyer either knows or strongly suspects that a client is engaged in either criminal or fraudulent activity:

- Rule 1.2(d) prohibits lawyer from advising a client where lawyer "knows" conduct is criminal or fraudulent.
- "[w]here facts known to the lawyer establish a high probability that a client seeks to use the lawyer's services for criminal or fraudulent activity, the lawyer has a duty to inquire further to avoid advising or assisting such activity."
- Ongoing duty to inquire, and if client refuses, to withdraw under Rule 1.16.

Going a step further, the ABA formally amended Rule 1.16(a), as well as Comments 1, 2, and 7 in 2023. Rule 1.16(a) now imposes an affirmative duty on lawyers to investigate the client's bonafides both before and during the representation:

> *A lawyer shall inquire into and assess the facts and circumstances of each representation to determine whether the lawyer may accept or continue the*

[26] See Report of the American Bar Association Task Force on Corporate Responsibility at 22 (March 31, 2003), available at http://www. abanet.org/buslaw/corporateresponsibility /final_report.pdf.

[27] *U.S. Officials Still Considering AML Rules for Attorneys,* ACAM moneylaundering.com/news, May 16, 2024.

> *representation*. Except as stated in paragraph (c), a lawyer shall not represent a client or, where representation has commenced, shall withdraw from the representation of a client if:
>
> (4) *the client or prospective client seeks to use or persists in using the lawyer's services to commit or further a crime or fraud, despite the lawyer's discussion pursuant to Rules 1.2(d) and 1.4(a)(5) regarding the limitations on the lawyer assisting with the proposed conduct.*

ABA offered additional guidance regarding amended Rule 1.16(a) by way of ABA Formal Opinion 513 in August 2024. Specifically, Opinion 513 clarifies that, before accepting representation, lawyers must conduct a reasonable, risk-based inquiry to determine the risk of assisting in a crime or fraud. In doing so, "[t]he lawyer need not resolve all doubts," and "if some doubt remains even after the lawyer has conducted a reasonable inquiry, the lawyer may proceed with the representation as long as the lawyer concludes that doing so is unlikely to involve assisting or furthering a crime or fraud." If the lawyer cannot so conclude, they must decline or withdraw from the representation. This duty remains ongoing throughout the course of the representation.

The lawyer must "[i]nquire into and assess the facts of each representation to avoid advising or assisting a client in conduct the lawyer knows to be criminal or fraudulent." According to Opinion 513, amended Rule 1.16 does not mean the lawyer must serve as "gatekeeper," but it does mean the lawyer must inquire using a "risk-based approach," meaning the inquiry is based on the "risk that the current or prospective seeks to use or persists in using the lawyer's services to commit or further a crime or fraud." The required scope and depth of inquiry will vary by client, depending on the nature and extent of the risk. In doing so, amended Rule 1.16 incorporates the concepts of "reasonableness and proportionality."

Opinion 513 provides five factors "a lawyer might consider" in determining the scope of their investigation:

- The identity of the client;
- The lawyer's experience and familiarity with the client;
- The nature of the requested legal services;
- The relevant judications involved in the representation;
- The identities of those depositing funds into, or receiving funds from, the lawyer's trust account, or any other accounts where client funds are held.

So what might this look like in practice? At a minimum, a reasonable inquiry might require asking (and obtaining answers to) the following questions:

- Who is the client (i.e., individual, corporation, or both)?
- Where is the client located? Where did they come from?
- Who are the beneficial owners of the client entity?
- What is the nature of the client's business/source of income?
- What is the scope of services that the lawyer is being asked to provide?

- Are there unusual aspects to the proposed representation (e.g., immediate use of lawyer's escrow account)?
- What publicly available information exists regarding the client?
- Has the lawyer received any third-party verification with respect to the client? (Be mindful, of course, of your duties of confidentiality under Rules 1.6 and 1.18)

Initial screening of clients can be accomplished through many electronic intake systems, such as InTapp Open. If you or your firm uses such a system for file openings, you should conform this initial screening to your firm's needs. For example, you might wish to check all prospective clients against the Specially Designated Nationals (SDN) List and the Non-SDN Consolidated Sanctions List.

After conducting an initial KYC investigation, lawyers should continue to monitor, based on risk, to identify suspicious activities. In doing so, consider using the OFAC site to keep aware of current sanctions.