



PROFESSIONAL COUNSEL®

Advice and Insight into the Practice of Law®

Third Party Vendors and Your Practice: How Allied Vendors Help Streamline Firm Operations

As with every other aspect of our lives, technology continues to redefine how lawyers practice and how law firms operate. In view of that basic premise, the pace of changing technology provides the opportunity for firms to regularly reassess their processes, operations, and systems. Routine system-wide assessments permit greater operational efficiency and productivity, improved client service, increased new client generation, and ultimately improved financial success. Moreover, a systematic reevaluation of law firm operations (which should typically occur at least once a year) is one tool out of many which firms have at their disposal to help minimize the risk of potential malpractice claims or claims of ethical impropriety. With pervasive and ever-evolving ethics rules, opinions, and legal malpractice precedent, this protocol becomes especially important.

This challenge creates a number of questions. The questions lawyers ask themselves should not be “Must I accept electronic payments?” or “Should my solo practice need an incident response plan?” Rather, those questions are better phrased as, “How do I improve my practice?” Or “How do I more efficiently track and follow up on my accounts receivable to free up more time to devote to clients?” “How can I organize my documents to be more accessible?” “Drastically reduce mistakes or human-led errors?” “Compile large amounts of data while seeing only what I need when I need it without missing a beat?” “How do I more securely communicate with my clients?” “Or keep my firm and clients protected against non-stop cyber risks and attack?” And of course, “How do I ensure that I get paid, and faster, for my work?”

Firms are increasingly rising to the challenge to become more technology-oriented, from both operational and client-service perspective.¹ This approach has been generated by both market demands as well as a growing recognition that part of a lawyer’s duty of competence includes knowledge of the benefits and risks of technology under Comment 8 of American Bar Association (ABA) Model Rule 1.1.² However, as demonstrated in the past year, the failure to navigate these challenges and changes may result in both unnecessary risk exposure as well as severe financial, professional, and reputational consequences for firms.³

To some extent, these questions may be better answered through the consistent evaluation and improvement of law firm operations.

The CNA [Lawyers Allied Vendor Program](#) offers solutions to help law firms navigate some of the challenges of managing a law firm as both a client service and a business, ultimately assisting with risk management measures. Some of the tools provided by partners with our Lawyers Allied Vendor Program include law practice management, cyber/data/communications security, payment platforms, e-discovery, time keeping, document management, and trial support, each of which provides enhanced abilities to automate and simplify the operations of a law firm in order to better serve clients.

¹ See Merken, S., *Orrick Tech Lab Spins Off First Independent Product, Pitching More Client Control*, Reuters Legal/Westlaw Today, (Apr. 13, 2021); see also Patrice, J., *Tech Company Spins Off From Biglaw Roots*, Above the Law, (Apr. 13, 2021).

² See ABA Model Rule of Professional Conduct 1.1, Comment [8] (2020).

³ Salvatore, C., *Alex Jones Atty Suspended Over ‘Stunning’ Discovery Leak*, Law360, (Jan. 6, 2023).

Law Practice Management

One such essential for today's legal market is law practice management (LPM) software. Although LPM programs have been available for many years, the services and benefits provided by contemporary cloud-based LPM software have been touted as a "game-changer" for the legal profession creating total flexibility for lawyers to access, track, and manage their firm's data from anywhere at any time.⁴ Since their very first offerings more than a decade ago, providers of LPM software have expanded into a burgeoning market catering to lawyers and the unique legal and ethical requirements of operating a practice. This growth has extended recently to practice-specific LPM software, such as LPM for intellectual property practices, which inherently include myriad deadlines and close interconnection between matters. Although specific features and strengths vary across LPM providers, many often focus on an "all-in-one" approach, whereby firms may integrate document management, timekeeping, trust account and business accounting, payment processing, and secure communications portals within one system. By housing many operational functions under one roof, firms are better able to track work performed across individual clients or client matters, as well as across workloads more generally firm-wide.

One other function offered by many LPM providers is the ability to communicate with clients through a secure, confidential client portal. In today's market, clients are increasingly eager to communicate with their lawyers via text message, about both mundane and highly sensitive topics. However, lawyers recognize the myriad issues that arise through sending text messages to clients, with privilege and confidentiality concerns as paramount.⁵ Although no form of communication is 100% secure, certain types offer more security features than others (e.g., requiring log in credentials, multi-factor authentication). Many LPM providers offer capabilities to communicate with clients, including both computer and mobile app accessibility, and permitting lawyers and clients to contact one another almost as easily as text messaging, but with enhanced security measures.

Payment Platforms

Lawyers also should review their payment processing systems and consider whether their current system adequately, efficiently, and securely addresses their needs. Research and surveys informing us that our society continues to move towards a "cashless" state are no longer as attention grabbing as they once were close to a decade ago. The data continues to demonstrate that more people – 41% – report using no cash for their typical weekly purchases.⁶ Based on those trends, it is clear that firms looking to attract a growing set of the population as new clients must adapt to these new payment methods. This issue of acceptable forms of payment for legal fees continues to receive numerous inquiries from lawyers seeking to remain compliant with their ethical duties (e.g., a recent Florida ethics opinion approving electronic funds as an acceptable method for payments into trust accounts⁷). In addition, society's shift towards electronic payment methods has resulted in an increased risk of theft and fraud through cyberattacks. In attracting those new clients featuring cashless payment methods, lawyers also must adhere to an ethics code which has largely remained impervious to market changes, requiring strict use, maintenance, disbursement, retention, and accounting of client funds.

Online payment platforms and processors can help simplify the payment process while permitting firms to expand their offerings to attract new clients in a secure environment. Payment processors for the legal market often provide tools designed to collect payments via multiple methods, including credit cards, which work in conjunction with firm operating and client trust accounts. This synergy often works to streamline the process, eliminating cumbersome processing hurdles in an attempt to comply with the rules regarding client funds and legal fees. The lawyer and the firm will remain obligated to ensure that payments are made, held, and received in a manner consistent with ABA Model Rules 1.5, 1.15, and 1.16. However, online legal payment processors create the ability to: i) to more easily and efficiently review funds coming in and out, ii) provide and schedule invoices to clients on a timely basis, and iii) pull accounting records for trust or IOLTA accounts when needed, all actions which may otherwise take up more valuable time and resources for lawyers.

⁴ Black, N., *The Ins and Outs of Law Practice Management Software*, ABA Journal. (Jan. 11, 2019).

⁵ Bethune, S., *How to Text Your Client, And Other Low-tech Things A Lawyer Needs to Know*, ABA TYL Magazine. (2021)

⁶ Faverio, M., *More Americans are Joining the 'Cashless' Economy*, Pew Research Center. (Oct. 5, 2022).

⁷ See Fla. Ethics Op. 21-2 (March 2021)

Cyber Security

Another significant area that law firms should consider is fortifying their data and cyber security. As recent numbers suggest, law firms continue to be targets for cyber and data attacks. Notably, the size of the law firm has increasingly been irrelevant, as hackers proceed to target firms of smaller sizes which may have considered themselves too “small” to be targeted for cyberattacks. Nevertheless, the large amount of sensitive and valuable data law firms maintain, often for mandated extended periods, represent a boon to criminal actors seeking to exploit loopholes in firms’ cybersecurity defenses. As one example, firms have reported increasing incidents of wire transfer fraud, a scheme whereby a scammer poses as a trusted source, typically by email, and requests an immediate transfer of electronic funds in transactions where they know the lawyer and clients and/or third parties are already scheduled to exchange funds. This scheme often occurs in residential or commercial real estate matters, with cyber attackers gaining access to one or multiple email accounts in order to send an email to the legitimate parties to the transaction which contains a fraudulent or inaccurate account number which is under the control of the criminal actor.⁸

Although lawyers are aware of the increasing risks associated with cyberattacks, a sizeable proportion of lawyers continue to be unprepared. The ABA’s Techreport 2022 revealed that approximately 58% of lawyers who responded did not have any incident response plan to manage cyberattacks or intrusions, with only 9% of solo practitioners reporting having such a plan.⁹ Implementing an incident response plan, a step-by-step procedure to deploy in the immediate aftermath of a cyberattack in order to protect both the firm and its clients, represents both sound practice and an alignment with ABA Formal Opinion 483, which describes lawyers’ ethical obligations following a data breach.¹⁰ There are several third party providers who specialize in assessing cyber risk specifically for the legal market. These providers often assist with cyber security assessments from both an internal and external perspective, readiness in the event of an attack, simulated phishing attacks to demonstrate real-world experiences, as well as security management. As with other third party providers, the specific functionalities may vary. However given the threat of cyberattacks against law firms of all sizes and the large number of lawyers who may not have taken action for one reason or another, cybersecurity vendors are available to craft unique responses for law firms of various sizes and needs.

Conclusion

Irrespective of the time of year or business cycle, lawyers should commit to an in-depth re-evaluation of their operations at least once a year – to determine what works, what doesn’t, and what may be improved. Technological advancements not only enable firms to regularly do so, but ethical and legal obligations also require lawyers to routinely assess their practice and operations in line with those advancements.

Lawyers should note that irrespective of the vendor(s) with whom they contract, they are still responsible for performing a reasonable amount of research and diligence into all external third party vendors, under ABA Model Rules 1.6 and 5.3, to ensure that the external providers are compatible with ethical obligations. This procedure may include considering certain factors, such as the “education, experience, and reputation of the non-lawyer, the nature of the services involved, the terms of any arrangements concerning the protection of client information, and the legal and ethical environments of the jurisdictions in which the services will be performed, especially with respect to confidentiality.”¹¹

Many of these tools and services are offered within the CNA Lawyers Allied Vendor Program, which includes the following:

- Court, Record Retrieval and Trial Support
- Cybersecurity
- Data & Communications Security
- Docketing, Calendaring & Case Watching
- Document Management
- eDiscovery
- IP Solutions
- New Business Intake, Conflict Management & Information Security
- Online Payment Platforms
- Law Practice Management Software

When performed and employed correctly, these routine operational maintenance checks and external third party vendors will not only enable firms to remain compliant with evolving duties owed to clients but will also help minimize risk exposure and simultaneously support an efficient and growing business.

⁸ Ginty, P., *Wire Transfer Fraud: A Growing Threat to Law Firms*, CNA Professional Counsel, (June 17, 2021).

⁹ See ABA TechReport 2022 (Nov. 2022).

¹⁰ See ABA Formal Op. 483 (Oct. 2018).

¹¹ ABA Model Rule of Professional Conduct 5.3, Comment [3] (2020).

This article was authored for the benefit of CNA by:

Christopher Heredia

Christopher Heredia is a Risk Control Consulting Director for CNA's Lawyers Professional Liability Program. He is responsible for developing content for CNA's Risk Control services by providing guidance to CNA's insureds on risk control and professional responsibility-related issues. Prior to joining CNA, Chris was an attorney with Am Law 100 firm in Chicago where he focused his practice in legal ethics, law firm risk management, and commercial litigation. Prior to his time in private practice, Chris served in the public sector, first as an Assistant State's Attorney with the Cook County State's Attorney's Office in Chicago, and later as Litigation Counsel for the Illinois Attorney Registration and Disciplinary Commission where he worked to regulate the legal profession in Illinois. He is admitted to practice in Illinois, the U.S. District Court for the Northern District of Illinois, and the U.S. Supreme Court.

About CNA Professional Counsel

This publication offers advice and insights to help lawyers identify risk exposures associated with their practice. Written exclusively by the members of CNA's Lawyers Professional Liability Risk Control team, it offers details, tips and recommendations on important topics from client misconduct to wire transfer fraud.

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com

Disclaimer: The author's opinions are their own and have not necessarily been adopted by their employers. The purpose of this article is to provide information, rather than advice or opinion. The information it contains is accurate to the best of the author's knowledge as of the date it was written, but it does not constitute and cannot substitute for the advice of a retained legal professional. Only your own attorney can provide you with assurances that the information contained herein is applicable or appropriate to your particular situation. Accordingly, you should not rely upon (or act upon, or refrain from acting upon) the material herein without first seeking legal advice from a lawyer admitted to practice in the relevant jurisdiction.

These examples are not those of any actual claim tendered to the CNA companies, and any resemblance to actual persons, insureds, and/or claims is purely accidental. The examples described herein are for illustrative purposes only. They are not intended to constitute a contract, to establish any duties or standards of care, or to acknowledge or imply that any given factual situation would be covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice. "CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporations subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities. Copyright © 2023 CNA. All rights reserved. Published 2/23.

