PROGRAM MATERIALS
Program #3615
January 29, 2026

Scam Typologies and Their Significance for Legal Professionals

Copyright ©2026 by

- Alex Kulikov, M.S., CFCI, CFCS, GAAP, PMP - Expert CA
- Ari Zahavi, J.D. - California Technical Media

All Rights Reserved.
Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

EXPERT CA:

SCAM TYPOLOGIES WEBINAR – CLE SUBMISSION PACKET

Prepared for: Celesq, AttorneysED Center

Prepared by: Alex Kulikov, Expert CA / MS / CFCI / CFCS / GAAP / Forensic Expert

Date: January 15, 2026

PROGRAM TITLE

Scam Typologies and Their Significance for Legal Professionals

PROGRAM DESCRIPTION

Legal professionals are increasingly targeted by sophisticated scams that exploit trust, authority structures, predictable workflows, and the unique responsibilities lawyers hold over confidential information and client funds. This Continuing Legal Education (CLE) program provides an expert-level overview of modern scam typologies- including business email compromise, fraudulent check schemes, AI-driven deepfake impersonation, tech-support malware attacks, vendor/court impersonation, and ransomware, as they apply specifically to legal practice.

Participants will learn how to identify early warning signs, understand the underlying psychological and technological mechanisms that make these scams effective, and implement internal controls that satisfy ethical duties under American Bar Association (ABA) Model Rules 1.1, 1.6, 1.15, and 5.3. Case law, ethics opinions, and regulatory guidance are integrated throughout to provide legal professionals with a framework for both prevention and compliance.

LEARNING OBJECTIVES

By the end of the program, participants will be able to:

1. Define a scam, identify and explain the primary scam typologies that target attorneys and law firms, including business email compromise, check fraud, tech support scams, and deepfake impersonation.
2. Recognize how scams directed at legal professionals differ from general consumer scams, focusing on workflow exploitation, ethical pressure points, and authority-based impersonation.

3. Evaluate the ethical implications under the American Bar Association (ABA) Model Rules, including duties of confidentiality, technological competence, supervision, and safeguarding client property.
4. Analyze some key cases and insurance disputes related to scam-induced losses, understanding how courts treat voluntary transfers and social engineering attacks.
5. Highlight best practices for prevention, implement effective internal controls within law firms, including dual authorization, multi-factor authentication, call-back verification, secure client portals, and staff training protocols.
6. Develop an incident response plan that meets regulatory expectations and minimizes client harm during scam-related events.

TIMED AGENDA (60-Minute CLE Program)

00:00 - 5:00 - Introduction and Overview

- Learning objectives
- Rise of global scam operations
- Why the legal profession is a high-value target
- Impact on client trust, financial security, and institutional integrity

5:00 - 10:00 - Defining Scams and Key Legal Distinctions

- Difference between scams and fraud
- Authorized vs. unauthorized transactions
- Why the distinction matters for attorney liability and insurance

10:00 - 20:00 - Modern Scam Landscape and Technology Drivers

- AI-powered impersonation
- Malware, spoofing, RATs, credential stuffing
- Screen-scraped websites and deepfake videos
- Growth trends and illustrative data

20:00 - 30:00 - How Scams Target Lawyers Differently

- Workflow mimicry (real estate closings, settlements, escrow)
- Hierarchical exploitation (fake partner instructions)
- Exploiting ethical obligations (fake emergencies)
- Psychological pressure points unique to legal practice

30:00 - 40:00 - Scam Typologies Affecting Law Firms

- Business email compromise (BEC) and business identity compromise (BIC)
- Anatomy of a BEC attack
- Check and trust-account fraud
- Technology-enabled Threats
    - Tech support and remote-access infiltration
    - Vendor / court / bar impersonation
    - Ransomware extortion
    - AI-enhanced deepfake deception

40:00 - 45:00 – Where do controls fail?

- Training
- Dual Control
- Multi-factor authentication
- Verifications
- Insider risk

45:00 – 50:00 – Ethical duties related to scams

- American Bar Association (ABA) Model Rules
    - Rule 1.1
    - Rule 1.15
    - Rule 1.6
    - Rule 5.3

50:00 - 57:00 - Best Practices, Internal Controls and Response Plan

- People, Process, Technology
- Mandatory verification procedures
- Dual-person wire approvals
- MFA and secure communication portals
- Staff training and phishing simulations
- Incident response and client notification protocols

57:00 - 60:00 - Q&A and Wrap-Up

PRESENTER BIOGRAPHY

Mr. Alex Kulikov is a Master of Science, Certified Financial Crimes Investigator, and Principle of Expert CA, with nearly 30 years of experience in forensic examination, white-collar crime investigations, and complex financial analysis. As a trusted consulting expert across financial services, real estate, fintech, construction, healthcare, technology and other sectors, Mr.

Kulikov has provided expert testimony in state and federal courts and served over 200 clients worldwide in matters related to internal and external fraud risk assessments, due diligence, money-trail reconstruction, cryptocurrency fraud analysis, contract dispute assessments, corruption investigations, and more. Mr. Kulikov has contributed to the advancement of financial crime prevention through advisory board service, frequent speaking engagements, and serving on the Executive Board as the Vice President and Chairman of the Education Committee of the National Forensic Expert Witness Association.

COURSE MATERIALS INCLUDED

Participants will receive the following supplementary materials:

- Scam Typologies CLE Submission Handout (30 pages, double-spaced)
- References to Statutes, Rules and Regulations, Cases and Reports
- 26-Page Scam Typologies Presentation Slide Deck, including Interactive Hypotheticals
- The Federal Reserve Toolkit – How Scams Occur and Why You Should Care About Scams

CONFLICT-OF-INTEREST DISCLOSURE & LEGAL DISCLAIMER

The presenter confirms they have no financial interest, external sponsorship, or conflict of interest related to the subject matter of this CLE program.

The presentation is provided for educational purposes and general information on legal matters and does not, and is not intended to constitute an expert opinion, legal advice or an expert-client relationship. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this presentation.

COPYRIGHT DISCLOSURE

© Expert CA. This content is protected under US Copyright (17 U.S.C. 201 et al.) and other federal law and shall not be published, reproduced, displayed or otherwise utilized by any person or entity whatsoever without prior consent of Expert CA. Violation of Expert CA's intellectual property rights will be prosecuted to the full extent of the law.

CLE Presentation: Scam Typologies and Their Significance for Legal Professionals

Submission Handout

Table of Contents

I. Introduction

Scams represent one of the most rapidly expanding threats to modern society, affecting individuals, businesses, and institutions at every level. While deceptive practices have existed for centuries, the scale, sophistication, and psychological precision of contemporary scams distinguish them sharply from prior years. As this presentation explains, scams today involve advanced social engineering methods, malware deployment, remote access tools, Artificial Intelligence (AI)-based voice spoofing and impersonation tactics, fake websites, and the coordinated efforts of global criminal networks capable of operating at unprecedented scale and anonymity. This evolution has caused billions of dollars in losses, enormous emotional damage, and severe disruption to business operations.

Legal professionals are increasingly at the center of this threat environment. As custodians of client funds, confidential information, and sensitive transactional workflows, lawyers offer criminals a unique combination of high-value targets and predictable operational patterns. Criminal enterprises deliberately study the practices of law firms- including personal identifying information, litigation strategy, protected client communications in trust account transactions, real estate and Mergers &Acquisitions (M&A) closings, settlement distributions, probate transfers, and escrow procedures, to design scams that mimic legitimate communications and exploit the legal profession's inherent time pressures and trust-based relationships.

This presentation synthesizes the typologies, behavioral patterns, and technological enablers of scams, integrating legal analysis, ethical frameworks, case law, and professional standards. It further examines how scammers target legal professionals differently from the

general public, why lawyers face greater financial and ethical risks, and how law firms can fortify their defenses in an increasingly hostile digital environment.

II. Defining Scams and Their Legal Significance

A functional understanding of scams begins with the precise terminology. The Federal Reserve's industry work group[1], recognizing confusion in public and professional discourse, established an operational definition that distinguishes scams from crimes such as fraud, identity theft, and unauthorized access. According to that definition, scams involve intentional deception whereby the victim is manipulated into *authorizing* the transfer of money, disclosing sensitive information, or granting access to the systems or accounts.

This distinction between scams as *"authorized"* transactions and fraud as *"unauthorized"* transactions carries significant legal consequences, including professional liability exposure, regulatory reporting obligations and liability related to trust account obligations. Many scam victims- including law firms, approve payments themselves under the influence of fraudulent instructions. Since the victim voluntarily initiates the transfer, financial institutions may deny reimbursement, cyber insurance coverage may be limited or nonexistent, and liability may fall on the professional who conducted inadequate verification.

For lawyers, the stakes are even higher. A scam-induced transfer may constitute mishandling of client trust funds, violation of fiduciary duties, or breach of the duty of

[1] The Federal Reserve uses various industry work groups and task forces, often convened to collaborate with financial institutions on developing standards and improving security (like fraud definitions). https://www.frbservices.org

technological competence under American Bar Association (ABA) Model Rule 1.1.[2] Regulators increasingly expect lawyers to recognize common scam indicators and implement internal controls to prevent such losses. Thus, understanding the structure and nature of scams is indispensable not only for risk mitigation but also for fulfilling professional obligations.

III. The Modern Scam Landscape

The sophistication of scams has escalated dramatically in recent years. According to Federal Trade Commission (FTC) reports, scams inflict billions of dollars in global losses annually[3], though the true figures are substantially higher due to underreporting caused by embarrassment, confusion, or fear of consequences. Scammers exploit universal human emotions- such as trust, urgency, fear, hope, and greed, through carefully designed psychological scripts intended to override rational decision-making.

At their core, modern scams rely on two forces: technological capability and human vulnerability. Digital communications such as phishing emails, smishing messages, spoofed phone calls, and fraudulent websites provide inexpensive and highly scalable channels for criminals. At the same time, social engineering techniques manipulate victims into believing the urgency or legitimacy of the communication. Criminals often impersonate trusted institutions,

---

[2] American Bar Association Model Rule 1.1: Competence, *Client-Lawyer Relationship*, A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/

[3] *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*, Federal Trade Commission (2025). https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

including banks, government agencies, employers, technology vendors, and- critically for this presentation, lawyers themselves.

Scams rarely occur in isolation. They frequently serve as gateways to additional crimes. A single phishing email may result in credentials theft, unauthorized account access, installation of remote access malware, or the compromise of the entire financial or legal workflows.

Ransomware attacks, in particular, can immobilize entire law firms, interrupt client representation, and expose confidential information. The interconnected nature of modern scams underscores the need for comprehensive prevention strategies, especially in legal environments where confidentiality and fiduciary responsibility are critical.

IV. Why Scams Matter to Legal Professionals

Lawyers occupy a fiduciary role that places them in a vulnerable position while simultaneously imposing heightened responsibility for preventing scams. Unlike many other professionals, attorneys are entrusted with client property, including substantial sums of money held in trust or escrow accounts, and are ethically obligated to safeguard those assets with the highest degree of care. In addition to handling trust and escrow accounts, lawyers serve as custodians of highly sensitive and privileged information, ranging from personal identifying data and financial records to litigation strategies, trade secrets, and confidential business negotiations. They also act as central coordinators in complex, high-value transactions, frequently serving as the intermediary among banks, counterparties, regulators, and clients. This combination of financial access, informational authority, and transactional control creates a powerful incentive

for criminal actors, who recognize that compromising a single attorney or law firm can yield immediate financial gain as well as valuable intelligence for future exploitation.

The structure of legal practice further amplifies this risk because many legal workflows are predictable and repeatable, making them vulnerable to imitation. Criminals invest time studying how lawyers communicate, how transactions progress, and when key decisions or transfers typically occur. In real estate transactions, for example, attorneys routinely handle closing funds and exchange wire instructions under tight timelines, often with multiple parties involved and frequent last-minute adjustments. Similarly, in mergers and acquisitions, settlement negotiations, probate matters, and large commercial disputes, it is not unusual for payment instructions to change close to a deadline due to regulatory requirements, financing issues, or clients' requests. Scammers exploit these realities by inserting fraudulent instructions at precisely the moment when lawyers expect legitimate changes. By impersonating lenders, brokers, investment bankers, or even the clients themselves- often using compromised email accounts or convincingly spoofed addresses, criminals create communications that appear routine, legitimate and authoritative. Because attorneys are accustomed to rapid decision-making in these contexts and are often under pressure to meet closing dates or court-imposed deadlines, they may execute transfers or release information before independently verifying the authenticity of the request.

In addition to these transactional vulnerabilities, attorneys operate under evolving professional standards that impose explicit duties related to confidentiality and technological competence. Modern rules of professional conduct require lawyers not only to protect client confidences in a traditional sense but also to understand the technological risks associated with electronic communications, digital storage, and online transactions. When an attorney falls

victim to a scam, the consequences frequently extend beyond a single transaction or client. A successful phishing attack or malware installation can expose entire law firm's email systems, document repositories, and case management platforms, potentially compromising multiple matters simultaneously. Such breaches may result in the disclosure of privileged communications, loss of strategic advantage in litigation, or exposure of sensitive client data, triggering reporting obligations and client notification requirements.

The harm caused by scams in the legal context is therefore multidimensional. Financial losses may affect trust account balances and require attorneys or firms to absorb or remediate shortfalls. Clients may lose confidence in the attorney's ability to protect their interests, leading to reputational damage that can be difficult to repair in a profession built on trust and credibility. Regulatory authorities may initiate investigations into whether the attorney exercised reasonable care, maintained adequate safeguards, and properly trained and supervised staff. In some cases, clients may pursue malpractice claims or disciplinary complaints, alleging that the lawyer failed to meet ethical and professional standards. These consequences elevate scams from isolated operational incidents to serious threats that can jeopardize a lawyer's practice, professional standing, and long-term reputation.

V. How Scams Target Legal Professionals Differently

Scams that target legal professionals differ in significant and consequential ways from those aimed at the general public because they are deliberately engineered to mirror the structure, language, and pressures of legal practice. Criminals who focus on lawyers do not rely on generic mass-marketing tactics or hard-to-believe offers. Instead, they design schemes that replicate

legitimate legal communications, exploit the hierarchical nature of law firms and legal departments, and manipulate the professional and ethical obligations that govern attorneys' conduct. Scammers understand that lawyers routinely handle large sums of client money, work under intense time constraints, and depend on trust-based relationships with clients, opposing counsel, financial institutions, and colleagues. These characteristics create an environment in which a well-timed and credible deception can succeed with devastating consequences.

One of the most effective strategies used against legal professionals is the impersonation of authority figures within the law firm. Criminals frequently pose as managing partners, senior partners, general counsel, chief financial officers, or key clients whose instructions would ordinarily be followed without hesitation. Advances in generative AI have dramatically enhanced the credibility of these impersonations. Scammers can now produce highly realistic emails that mimic writing style and tone, create voice recordings that sound indistinguishable from a known individual, or even generate deepfake videos impersonating a partner or executive issuing urgent instructions. These communications often convey a sense of urgency, such as a directive to authorize a wire transfer before a deadline, release documents for a quick filing, or handle a confidential matter. Within hierarchical law firm environments, junior attorneys and staff may feel strong pressure to comply quickly, particularly when the request appears to come from a superior and carries an expectation of confidentiality or urgency.

Another way scammers target legal professionals is by exploiting the ethical duties that define the practice of law. Attorneys are trained to respond promptly to client emergencies, court deadlines, and regulatory developments. Criminals take advantage of this professional standard by fabricating crisis scenarios that demand immediate action. For example, a scammer may

claim that a client has been unexpectedly detained and needs bail funds transferred immediately, that a corporate transaction will collapse unless revised payment instructions are followed without delay, or that a court has issued an urgent order requiring immediate compliance. In some cases, scammers impersonate judges, court clerks, or government officials to add a sense of authority and legitimacy. Because lawyers are trained to prioritize client protection, court compliance, and risk mitigation, these fabricated emergencies create intense psychological pressure to act first and verify later, if at all.

The legal profession's heavy reliance on email communication further amplifies these risks. Email remains the primary tool through which law firms exchange drafts, settlement agreements, wire instructions, pleadings, and confidential client communications. As a result, email compromise is one of the most effective and damaging attack options against legal professionals. When criminals gain access to an attorney's email inbox- whether through phishing, credential theft, or malware, they often do not act immediately. Instead, they quietly monitor all communications over time, learning the details of the ongoing matters, identifying key players, and waiting for the optimal moment to strike. At a critical point, such as the day of a real estate closing or settlement distribution, the scammer inserts fraudulent instructions that appear entirely consistent with the surrounding email exchange. In addition to redirecting funds, criminals may harvest confidential documents, gather sensitive information for identity theft or extortion, or threaten to expose privileged materials unless a ransom is paid.

These targeted tactics highlight a fundamental difference between scams aimed at legal professionals and those directed at the general public. While consumer scams often rely on high-volume messaging, generic narratives, and indiscriminate targeting, scams against lawyers are

carefully researched, personalized, and specific to the case or matter. They are designed to blend into legitimate legal workflows and to exploit the ethical expectations, trust relationships, and operational pressures unique to the legal professionals. This strategic and tailored approach makes such scams far more difficult to detect and far more dangerous in their potential impact, underscoring the need for heightened awareness, training, verification protocols, and other safeguards.

VI. Scam Typologies Affecting Legal Practice

The typologies outlined in the above-mentioned FTC report provide a comprehensive framework for understanding scams targeting individuals and businesses. When applied to the legal profession, these typologies reveal several categories particularly relevant to attorneys and law firms.

A notable category is business email compromise (BEC), in which criminals impersonate clients or business partners to direct fraudulent transfers. BEC often involves spoofed email addresses or hacked accounts instructing lawyers to redirect settlement funds, change wire instructions for real estate or M&A closings and release escrow funds prematurely. This scheme is devastating in legal environments where attorneys regularly initiate large wire transfers and when trust funds must be disbursed promptly. Some notable features of BEC include high urgency of the messages in email communication, and "updated wire instructions to a new account due to audit delays" (as an example).

Check fraud represents another high-risk typology. Scammers send counterfeit checks that appear legitimate to law firms and then pressure victims to refund or transfer funds before

the check clears. Attorneys are especially vulnerable when the scam is framed as a settlement payment or retainer deposit. For instance, a “client” hires a law firm for a business dispute; the opposing party “settles immediately”; the law firm receives a large cashier’s check; the client insists funds must be quickly transferred; bank later flags the deposited check as fraudulent. When the fraudulent check bounces, the attorney may face ethical liability for the resulting trust account shortfall.

Technical support and remote access scams also increasingly affect law firms. Criminals impersonate technology vendors, claim that a device has been compromised, and instruct the victim to download remote access software. This enables criminals to seize control of computers, install malware, gain entry to document management systems (DMS), access email servers, confidential files and stored passwords. For a law firm, such unauthorized access may compromise entire document management systems and privileged communications.

Impersonation scams extend beyond vendors to courts, government agencies, and bar associations. Lawyers receive convincing but fraudulent notices about court e-filings, continued legal education (CLE) requirements, legal research providers, expert directories, process servers, Information Technology (IT) vendors, or legal license status. These notices are often delivered to attorneys via phishing links or spoofed renewal notices, prompting them to click malicious links or disclose sensitive credentials.

Artificial intelligence has introduced new scam typologies, including deepfake impersonations of senior attorneys. Federal Bureau of Investigation (FBI) has warned that Business Identity Compromise (BIC) represents an evolution in BEC by leveraging advanced techniques and new tools. Whereas BEC primarily includes the compromise of corporate email

accounts to conduct fraudulent financial activities, BIC involves the use of content generation and manipulation tools to develop synthetic corporate personas or to create a sophisticated emulation of an existing employee.[4]

These technologically sophisticated scams undermine traditional verification methods and exploit the authority structure within law firms. Scammers may use AI to clone the senior law firm partner's voice with a request to "authorize wire now" or "I am boarding a plane – do this immediately".

Deepfakes are extensively documented as a growing threat in numerous official reports and cybersecurity reviews from both government bodies and private industry firms, including the one by KPMG in 2025 indicating that 66% of cybersecurity professionals experienced a deepfake security incident in the past year, a 13% increase from the previous year.[5]

Finally, ransomware attacks represent one of the most destructive threats to law firms. Criminals encrypt firms' data and demand payment in cryptocurrency, threatening to leak client information if demands are not met. The legal and ethical consequences of such breaches are severe- including regulatory penalties and client lawsuits for data breach negligence, making ransomware prevention a central priority for legal organizations.

---

[4] Federal Bureau of Investigation, Private Industry Notification, March 10, 2021. https://www.ic3.gov/CSA/2021/210310-2.pdf

[5] KPMG LLP, *Deepfakes: Real Threat* (2025). https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/deepfakes-real-threat.pdf

VII. Technology-Enabled Threats

Technology-enabled threats play a central role in the modern scam ecosystem, and the FTC report referenced above underscores the variety and sophistication of the tools now deployed by criminal actors.

Techniques such as phishing and smishing allow scammers to send emails or text messages that convincingly imitate legitimate businesses, courts, financial institutions, or trusted individuals.

Caller ID spoofing enables criminals to disguise the originating phone number of a call so that it appears to come from a known client, a law firm office line, or even a government agency.

Malware and spyware are used to infiltrate computers and mobile devices, quietly stealing passwords, keystrokes, and sensitive documents over time.

Remote access trojans provide criminals with persistent, invisible control over a victim's device, allowing them to observe activity, intercept communications, and manipulate systems without detection.

Screen-scraped or cloned websites replicate the look and functionality of legitimate portals, such as online banking platforms, court filing systems, or document-sharing services, tricking users into entering credentials or financial information.

Subscriber Identity Module (SIM) card swapping and account takeover schemes exploit weaknesses in telecommunications systems to hijack phone numbers, intercept multi-factor authentication (MFA) codes, and gain access to email and financial accounts.

Credential stuffing and botnets automate the testing of stolen usernames and passwords across multiple platforms, enabling criminals to compromise numerous accounts at scale.

Together, these technologies dramatically increase scammers' ability to appear legitimate, operate efficiently on a massive scale, and conceal their identities and locations.

AI has amplified these threats to an unprecedented degree. Voice cloning technologies now require only seconds of recorded speech to replicate a person's voice with striking accuracy. In a legal context, this means that a scammer can convincingly impersonate a client, managing partner, or corporate executive in a phone call, urging an attorney or staff member to authorize a wire transfer or disclose confidential information.

Deepfake video technology extends this deception even further by recreating facial expressions, gestures, and speech patterns that appear authentic in real time or in recorded messages. A video call showing a known individual may no longer provide reliable assurance of identity.

At the same time, AI-generated text has reached a level of sophistication that allows scammers to craft emails that mirror the tone, formatting, and vocabulary of genuine legal communications, eliminating many of the traditional red flags that once helped recipients identify fraudulent messages. These AI-driven capabilities allow scams to be highly personalized, adaptive, and convincing, making them especially dangerous in professional environments built on trust and familiarity.

Law firms are particularly exposed to these technology-enabled threats because many lag behind other industries in cybersecurity maturity. Small and midsized law firms, in particular, often operate without dedicated IT staff, rely on outdated computer systems, or permit inconsistent security practices across laptops, mobile devices, and remote work environments. Even larger firms may struggle to enforce uniform security configurations or to keep up with

rapidly evolving cyber threats. These gaps create attractive entry points for sophisticated scammers, who understand that compromising a single device or account can provide access to a law firm's broader network. Once inside the computer network, criminals may gain visibility into ongoing matters, download privileged documents, intercept sensitive communications, or manipulate financial transactions involving client funds. From the perspective of a scammer, breaching a law firm offers an unusually high return on investment: access to confidential client data, insight into complex transactions, and opportunities to divert significant sums of money. This reality explains why technologically advanced scam operations increasingly view law firms not as peripheral targets, but as high-value gateways into financial systems and sensitive information flows.

VIII. Psychological and Behavioral Dynamics Behind Scams

Scams succeed not only because of technological sophistication but because they are carefully designed to exploit fundamental psychological and behavioral tendencies that influence human decision-making. Criminals deliberately manipulate emotions such as fear, urgency, sympathy, excitement, and the desire for financial security or opportunity in order to override rational analysis. When an individual experiences heightened emotional arousal, cognitive processing tends to narrow, and attention becomes focused on resolving the perceived threat or opportunity as quickly as possible. In these moments, people are less likely to engage in deliberate verification, question assumptions, or seek independent confirmation and advice. Instead, they rely on intuition and habitual responses, which scammers have studied extensively and learned to exploit with precision.

Legal professionals are particularly susceptible to these dynamics because of the psychological pressures inherent in legal practice. Attorneys routinely manage demanding caseloads, balance multiple client matters, and work within rigid deadlines imposed by courts, regulators, and transactional timetables. The expectation to respond promptly and competently is deeply imbedded in professional culture, and delays can carry real consequences for clients. As a result, lawyers often develop a habit of rapid decision-making, particularly when communications appear routine or urgent. When an email, call, or message seems to originate from a client, opposing counsel, a court, or a senior colleague, attorneys may instinctively prioritize immediate action over careful scrutiny, especially if the communication aligns with an ongoing matter or anticipated development.

The nature of legal work also reinforces patterns of trust that scammers are targeting to exploit. Lawyers depend heavily on established professional relationships and shared norms of reliability and authority. When a communication appears to come from a familiar source or someone in a position of authority, such as a managing partner, judge, or long-standing client, it triggers an automatic assumption of legitimacy. Criminals intentionally craft messages that fit within these expectations, using correct terminology, referencing real matters, and mimicking established communication styles. This familiarity lowers skepticism and increases the likelihood of compliance, particularly when combined with time pressure or emotional cues suggesting that delay could cause harm.

Another critical factor is the professional identity many lawyers develop over time. Attorneys are trained to analyze complex information, spot inconsistencies, and exercise judgment under pressure. This training often fosters a strong sense of competence and control,

which is essential for effective legal representation but can paradoxically increase vulnerability to deception. Lawyers, like other highly trained professionals, may believe they are unlikely to be fooled by scams and therefore may not apply the same level of caution they would advise to clients. Criminals exploit this cognitive bias by designing scams that appear highly tailored, technically sophisticated, and contextually accurate. The apparent complexity and customization of the communication can reinforce the victim's belief that the message is legitimate, discouraging further verification and creating a false sense of confidence.

These psychological and behavioral dynamics highlight why scam prevention cannot rely exclusively on awareness of technological threats. They highlight the need for ongoing training that addresses not only how scams work, but why they work and succeed. Simulation exercises that replicate realistic scenarios help attorneys and staff recognize emotional triggers and practice pausing before acting. Equally important is fostering a law firm's culture in which verification is encouraged and normalized. Lawyers and staff should feel comfortable questioning unusual requests, even when they appear to come from senior figures or trusted clients, without fear of appearing incompetent, uncooperative, or overly cautious. By acknowledging human vulnerability and embedding verification into everyday practice, legal organizations can significantly reduce the effectiveness of scams that rely on psychological manipulation rather than technical intrusion.

IX. Case Law and Regulatory Implications

Courts increasingly address disputes arising from scam-induced losses, particularly where insurance coverage is at issue. In *Great American Insurance Co. v. AFS/IBEX Financial*

Services, Inc.,[6] the court held that a voluntary transfer of funds induced by deception did not qualify as a direct loss under the applicable policy. This narrow interpretation of coverage is common in disputes involving business email compromise and other scam-based losses.

In *Realpage, Inc. v. National Union Fire Insurance Co. of Pittsburgh*[7] and *Door Sys., Inc. v. CFC Underwriting Ltd.*,[8] courts similarly concluded that impersonation schemes fall outside traditional crime coverage unless expressly included. These decisions underscore the importance of carefully reviewing policy language and securing endorsements that cover social engineering attacks.

Regulatory bodies have also established standards that must be followed by legal professionals. ABA Rules 1.1 and 1.6[9] emphasize that lawyers must adopt reasonable measures to protect against cyber risks, including the use of secure networks, encryption, and verification protocols. Other jurisdictions have issued similar guidance, interpreting technological competence as essential to fulfilling ethical obligations such as under *The State Bar of California's Formal Opinion 2015-193*.[10]

---

[6] *Great American Insurance Co. v. AFS/IBEX Financial Services, Inc.,* United States Court of Appeals for Fifth Circuit (2010). https://cases.justia.com/federal/appellate-courts/ca5/09-10262/09-10262-cv0.wpd-2011-03-16.pdf?ts=1410987480

[7] *Realpage, Inc. v. National Union Fire Insurance Co. of Pittsburgh*, No. 21-10299 (5th Cir. 2021). https://law.justia.com/cases/federal/appellate-courts/ca5/21-10299/21-10299-2021-12-22.html

[8] *Door Sys., Inc. v. CFC Underwriting Ltd.*, 2024 (Cal. Ct. App. June 3, 2024). https://www.stblaw.com/docs/default-source/publications/insurancelawalert_june2024.pdf

[9] American Bar Association Model Rule 1.6: Confidentiality of Information: (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

[10] State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193 on an attorney's ethical duties in the handling of discovery of electronically stored information (2015). https://www.calbar.ca.gov/sites/default/files/portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL.pdf

The legal system also considers the broader consequences of scam-related breaches. When privileged information is exposed, courts look at whether privilege is waived, whether sanctions apply, and how to balance the interests of clients whose confidentiality has been compromised. This rapidly evolving area of law demonstrates that scams are not merely operational risks but legal issues with significant implications.

X. Ethical Duties and Professional Liability

Ethical duties and professional liability are closely connected to scam prevention in modern legal practice, as the obligations imposed on lawyers increasingly include technological awareness and risk management. Attorneys are not only advocates and advisors; they are fiduciaries entrusted with protecting client information, property, and interests. As scams grow more sophisticated and digitally enabled, professional responsibility rules operate as a framework through which lawyers' conduct is evaluated when scam-related harm occurs.

Under Model Rule 1.6, lawyers have a duty to safeguard their clients' confidential information, a responsibility that now clearly extends to electronic communications and digital data. Protecting confidentiality in today's environment requires more than discretion in conversation or document handling; it demands reasonable technical and administrative safeguards against unauthorized access. If a lawyer falls victim to a phishing attack that exposes client emails, litigation strategies, or sensitive financial records, the analysis does not end with the fact that the lawyer was deceived. Regulators and courts increasingly ask whether the lawyer took reasonable steps to secure email systems, implemented multi-factor authentication (MFA), trained staff to recognize suspicious messages, and responded promptly once a breach was

suspected. A failure to adopt commonly accepted cybersecurity practices may be viewed as a breach of the duty of confidentiality, even when the underlying scam was sophisticated and well-disguised.

Model Rule 1.15[11] imposes a strict obligation on lawyers to safeguard client property, including funds held in trust or escrow accounts. Trust account rules are often enforced on a strict liability basis, reflecting the profession's concern for the protection of clients' money. When a scam results in the misdirection of trust funds- such as through fraudulent wire instructions or counterfeit settlement checks, the fact that the lawyer was tricked does not automatically excuse the loss. Disciplinary authorities may examine whether the attorney followed reasonable verification procedures, such as independently confirming wire instructions or delaying disbursement until funds were fully cleared. Even where the lawyer acted in good faith, a scam-infected trust account shortfall can still constitute a violation of Model Rule 1.15, exposing the attorney to discipline, restitution obligations, or both. This reality demonstrates why scams involving client funds present severe ethical and professional risks.

Model Rule 5.3[12] further expands a lawyer's responsibility by imposing duties to supervise non-lawyer assistants, including paralegals, legal assistants, administrative staff, and accounting personnel. In practice, many scam-related incidents originate with non-lawyer employees who handle emails, process payments, or manage trust accounts. When a staff

---

[11] American Bar Association Model Rule 1.15: *Safekeeping Property, Client-Lawyer Relationship.* https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property/

[12] American Bar Association Model Rule 5.3: *Responsibilities Regarding Nonlawyer Assistance, Law Firms and Associations.* https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/

member responds to a fraudulent email, installs malicious software, or authorizes a payment based on deceptive instructions, regulators often look to the supervising attorney to determine whether adequate training, policies, and oversight were in place. The failure of a paralegal or administrator to recognize a scam may therefore be attributed to the supervising lawyer if the firm lacked clear protocols, regular training, or proper supervision. This makes scam awareness, training and cybersecurity education not merely best practices, but ethical necessities under the rules governing supervision.

Beyond disciplinary exposure, scam-related incidents frequently give rise to professional liability claims when clients suffer financial loss, data exposure, or disruption to their legal matters. In evaluating malpractice claims, courts typically focus on whether the attorney acted reasonably under the circumstances. This inquiry may include whether the lawyer employed industry-standard verification procedures, whether the firm's staff were trained to identify common scam indicators, whether internal controls existed to prevent single-point failures, and whether the attorney responded appropriately once the scam was discovered. Courts may also consider whether the lawyer adhered to ethical guidance issued by bar associations regarding technological competence and cybersecurity. As scam activity continues to increase and digital threats become more widespread, courts are likely to set more explicit expectations for attorneys' conduct in technology-driven world.

Together, these ethical and liability considerations illustrate that scam prevention is no longer a choice or a matter of personal preference alone. It is an integral component of attorneys' professional responsibility. Lawyers are expected to anticipate the related risks, implement reasonable safeguards, and supervise both technology and personnel in a manner consistent with

their fiduciary obligations. As the legal profession adapts to evolving digital threats, ethical rules and liability standards will continue to shape how lawyers are judged when scams succeed, reinforcing the need for proactive, informed, and systematic approaches to prevention.

XI. Internal Controls and Best Practices for Law Firms

Effective mitigation of scam risks within law firms requires a comprehensive and coordinated approach that integrates appropriate policies, technological safeguards, and firm-wide reinforcement. No single control is sufficient on its own, because modern scams are adaptive and often exploit multiple weaknesses simultaneously. Law firms must assume that attempts at deception will continue occurring in the future. This requires that internal systems should be designed to slow decision-making at critical moments, require independent verification, and reduce the likelihood that a single error will result in a catastrophic loss.

At the work process level, mandatory verification protocols are among the most important defenses against scam-related financial losses. Law firms routinely process wire transfers, settlement disbursements, escrow payments, and other high-value transactions, often under time pressure. To counter this risk, firms should require independent confirmation of all financial transfer instructions using contact information that is already known and trusted, rather than relying on information contained in the same email or message that initiated the request. For example, when wire instructions are received by email, the firm should require a call-back to a verified phone number on file for the client, lender, or counterparty before any funds are released. This verification should be documented and, ideally, require approval from more than one individual. Dual authorization requirements for outgoing wires and trust account

disbursements can significantly reduce the risk of a successful scam by eliminating single points of failure and forcing a pause that allows inconsistencies to be detected. Test transfers in smaller amounts are also a good choice. Once the smaller transfer clears, the balance transfer may proceed.

Technological safeguards play an equally critical role in scam prevention. Multi-factor authentication should be implemented firm-wide for email, document management systems, financial platforms, and remote access tools. MFA makes it substantially more difficult for criminals to gain access to accounts even if passwords are compromised through phishing or malware.

Email authentication technologies, such as domain-based message authentication, reporting, and conformance protocols, help prevent spoofed emails from appearing legitimate and reduce the likelihood that fraudulent messages will reach mail inboxes.

Endpoint detection and response tools can identify suspicious activity on laptops and mobile devices, such as the installation of remote access trojans or unauthorized data transfers, allowing firms to respond before significant damage occurs.

Encryption of data at storage and in transmission protects client information even if systems are breached, while secure client portals reduce reliance on email for transmitting sensitive documents, settlement instructions, and financial information.

Ongoing education and training are essential to ensure that procedural and technical controls function effectively. Regular security awareness training helps attorneys and staff recognize common scam indicators, understand evolving threat tactics, and practice appropriate responses. Regular simulated phishing exercises are particularly valuable because they expose

employees to realistic scenarios in a controlled environment, reinforcing vigilance without real-world consequences. Training should not be limited to entry-level staff; partners and senior attorneys must also participate and set the tone from the top, as scammers frequently target individuals in positions of authority whose actions carry the greatest impact. By normalizing continuous learning around scam prevention, firms can reduce complacency and keep awareness aligned with the current threat landscapes.

Preparation for the inevitable incident is another critical component of law firms' best practices. Firms should develop and maintain incident response plans that clearly outline roles, responsibilities, and decision-making authority in the event of a suspected scam or breach. These plans should address how to contain the incident, preserve evidence, notify affected clients, communicate with financial institutions, and comply with any applicable regulatory or ethical reporting obligations. Having predefined procedures reduces confusion and delays during high-stress situations, when a quick and informed action is essential. Maintaining relationships with verified external cybersecurity vendors, forensic experts and investigators, insurance carriers, and legal ethics counsel further enhances law firms' preparedness by ensuring that expert assistance is immediately available when needed.

Finally, the effectiveness of all controls ultimately depends on the firm's culture. Lawyers and staff must feel empowered to question unusual or urgent requests, even when they appear to come from senior leadership, long-standing clients, or authoritative sources. Fear of appearing uncooperative, overly cautious, or incompetent can undermine verification efforts if employees hesitate to speak up. Leadership plays a crucial role in setting expectations by consistently reinforcing that verification is a professional obligation, not an inconvenience.

When firm leadership openly supports cautious behavior and treats near-misses as learning opportunities rather than failures, it encourages transparency and collective responsibility. A culture that prioritizes verification, open communication, and shared awareness strengthens resilience across the organization and significantly reduces the risk of deception, even as scam tactics continue to evolve.

XII. Broader Societal and Institutional Impacts

The impact of scams extends beyond individual victims or isolated law firms, reaching into the society as a whole and undermining trust in institutions that depend on reliability, integrity, and professional competence. As this review demonstrates, the proliferation of sophisticated scams contributes to a broader erosion of confidence in legal and financial systems, digital communications, and professional services. When people repeatedly hear of fraudulent transactions, data breaches, and impersonation schemes, they may begin to doubt the safety of online interactions, the reliability of electronic payments, and the ability of trusted professionals to protect clients' interests. This erosion of trust can have far-reaching consequences, including reduced participation in digital commerce, increased skepticism toward legitimate communications, and heightened anxiety about engaging with financial and legal systems.

The implications are particularly serious when lawyers- who serve as guardians of justice, fiduciaries of client interests, and key intermediaries in financial and legal transactions, fall victim to scams. The legal profession occupies a central role in upholding the rule of law and facilitating orderly economic and social interactions. When attorneys or law firms are compromised by scams, the harm is not limited to the immediate parties involved. Publicly

reported incidents of trust account theft, data breaches, or fraudulent transfers can weaken confidence in the legal system as a whole, causing clients to question whether their lawyers can truly safeguard their money, confidential information, and rights. For certain vulnerable groups, such as seniors, small business owners, or individuals navigating complex legal matters, this loss of trust may discourage them from seeking legal assistance at all, further widening gaps in access to justice.

Scams also have a direct and troubling connection to organized crime and other illicit activities. The proceeds generated through fraudulent schemes often serve as a primary funding source for sophisticated criminal networks engaged in money laundering, human trafficking, drug distribution, and cybercrime. Scam operations are frequently part of larger transnational enterprises that exploit both technological vulnerabilities and human behavior to generate steady revenue streams. Funds extracted from victims are rapidly moved through layers of accounts, cryptocurrency wallets, and shell companies, making recovery very difficult and enabling criminals to reinvest in more advanced tools, equipment and infrastructure. In this way, each successful scam not only harms its immediate victim but also strengthens criminal ecosystems that pose broader threats to public safety and economic stability worldwide.

Experts in white-collar crime prevention also play a critical role in disrupting these financial pipelines and mitigating their impact on society. Experts in the field are often in a position to identify red flags associated with suspicious transactions, unusual payment requests, or inconsistencies in client behavior. By following experts' recommendations, implementing strong internal controls, adhering to ethical obligations, and exercising vigilance in financial and transactional matters, attorneys can prevent their practices from being used as venues for illicit

funds' transfers. Experts also serve as educators and advisors to attorneys and their clients, helping them understand scam risks, verify communications, and adopt safer practices in their own operations. This advisory role extends the protective effect of scam awareness beyond the law firm itself and into the broader business and community environments in which clients operate.

Beyond individual representation, lawyers influence policy development and the evolution of legal frameworks designed to combat cybercrime and fraud. Through advocacy, participation in bar associations, and engagement with regulators, legal professionals contribute to shaping laws and regulations that address emerging threats, enhance reporting mechanisms, and strengthen enforcement tools. Attorneys also play a role in balancing the need for security with the protection of privacy, due process, and access to justice. In this sense, the legal profession is not merely a target of scams but a key factor in the collective response to these scams. By maintaining high standards of competence, integrity, and vigilance, lawyers help reinforce institutional trust and support resilience against the growing threat of sophisticated scams.

XIII. Conclusion

Scams represent an escalating and evolving threat to the legal profession, driven by the rapid advancement of technology and the deliberate exploitation of human psychology. As this analysis demonstrates, lawyers are not simply incidental targets; they are strategically selected because of their fiduciary responsibilities, their central role in financial and legal transactions, their reliance on predictable workflows, and their access to high-value client assets and sensitive

information. Criminal actors understand the legal profession's pressures, norms, and ethical commitments, and they design schemes that blend seamlessly into legitimate legal processes. As scam techniques become more sophisticated, personalized, and technologically advanced, the potential harm to clients, law firms, and the integrity of the legal system continues to grow.

The consequences of these threats extend far beyond isolated financial losses. Scam-related incidents can undermine attorney-client trust, expose confidential and privileged information, disrupt legal proceedings, and trigger disciplinary actions, malpractice claims, and regulatory scrutiny. They can also erode public confidence in the legal profession itself, particularly when lawyers- entrusted as guardians of client interests and officers of the court, are perceived as unable to protect funds or information. These risks prove that scam prevention is no longer a distant or hypothetical operational concern but a core component of a professional responsibility and ethical practice in the modern legal environment.

Addressing this challenge requires attorneys' deliberate effort and sustained response. Understanding scam typologies allows lawyers to recognize patterns, anticipate threats, and identify the red flags before harm occurs. Enhancing technological competence enables attorneys to assess the risks associated with digital communication, remote work, and electronic transactions and to make informed decisions about security measures. Implementing robust internal controls, including verification procedures, layered approvals, and secure communication channels, reduces the likelihood that a single mistake or moment of pressure will lead to catastrophic consequences. Equally important is fostering a culture of verification within law firms, where attorneys and staff are encouraged to pause, question, and confirm unusual requests without fear of appearing uncooperative or overly cautious.

Ultimately, the legal professional occupies a critical position in the broader effort to combat modern scams. Lawyers serve not only as potential targets but also as gatekeepers, advisors, and influencers who can disrupt criminal schemes, educate clients, and help shape effective policy responses. Through continuous vigilance, regular education, training and a commitment to ethical and technological competence, legal professionals can strengthen their own practices while contributing to the protection of clients, institutions, and the justice system as a whole. In doing so, they become an essential line of defense against the growing and increasingly sophisticated threat posed by modern scams.

XIV. References

Statutes

Computer Fraud and Abuse Act (1986). https://www.justice.gov/jm/jm-9-48000-computer-fraud

Rules and Regulations

American Bar Association (ABA) Model Rule 1.1: *Competence, Client-Lawyer Relationship*. https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/

American Bar Association Model Rule 1.15: *Safekeeping Property, Client-Lawyer Relationship.* *https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property/*

American Bar Association Model Rule 1.6: *Confidentiality of Information.* https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

American Bar Association Model Rule 5.3: *Responsibilities Regarding Nonlawyer Assistance, Law Firms and Associations.* *https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/*

State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193 on an attorney's ethical duties in the handling of discovery of electronically stored information (2015). https://www.calbar.ca.gov/sites/default/files/portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL.pdf

Cases

Door Sys., Inc. v. CFC Underwriting Ltd., 2024 (Cal. Ct. App. June 3, 2024). https://www.stblaw.com/docs/default-source/publications/insurancelawalert_june2024.pdf

Great American Insurance Co. v. AFS/IBEX Financial Services, Inc., United States Court of Appeals for Fifth Circuit (2010). https://cases.justia.com/federal/appellate-courts/ca5/09-10262/09-10262-cv0.wpd-2011-03-16.pdf?ts=1410987480

Realpage, Inc. v. National Union Fire Insurance Co. of Pittsburgh, No. 21-10299 (5th Cir. 2021). https://law.justia.com/cases/federal/appellate-courts/ca5/21-10299/21-10299-2021-12-22.html

Reports

Federal Bureau of Investigation, Private Industry Notification, March 10, 2021. https://www.ic3.gov/CSA/2021/210310-2.pdf

Federal Reserve. https://www.frbservices.org

Federal Trade Commission. ReportFraud. https://reportfraud.ftc.gov

KPMG LLP, *Deepfakes: Real Threat* (2025). https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/deepfakes-real-threat.pdf

New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024, Federal Trade Commission (2025). https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Expert CA

Scam Typologies and Their Significance for Legal Professionals

- Live Webcast CLE Presentation | Celesq AttorneysED Center | January 29, 2026
- Prepared by Alex Kulikov, MS, CFCI, CFCS, GAAP, PMP

Expert CA
© 2022-2026 All Rights Reserved

ALEX KULIKOV, MS, CFCI, CFCS, GAAP, PMP

- Certified Financial Crimes Investigator and Forensic Expert Witness;
- Over 29 years in risk management, white-collar crime prevention/detection, and litigation consulting;
- Provided expert consulting in over 30 state and federal court cases, civil and criminal, involving RICO, contract disputes, internal and external fraud, alter ego analysis, and crypto scams;
- Advisory experience with over 200 clients globally across financial, fintech, real estate, construction, health care, technology, gaming, food, and other sectors;
- Board Vice President and Chairman of the Education Committee of the National Forensic Expert Witness Association (FEWA).

Principal, Expert CA
t. 707-330-0054
e. alex@expertadvisors.us
w. https://expertadvisors.us

CONFLICT-OF-INTEREST DISCLOSURE & LEGAL DISCLAIMER

The presenter confirms they have no financial interest, external sponsorship, or conflict of interest related to the subject matter of this CLE program.

The presentation is provided for educational purposes and general information on legal matters and is not intended to constitute expert or legal advice or an expert-client relationship. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this presentation.

COPYRIGHT DISCLOSURE

© Expert CA. This content is protected under US Copyright (17 U.S.C. 201 et al.) and other federal law and shall not be published, reproduced, displayed or otherwise utilized by any person or entity whatsoever without prior consent of Expert CA. Violation of Expert CA's intellectual property rights will be prosecuted to the full extent of the law.

- What are the learning objectives?
- What is a scam?
- What is the modern scam landscape?
- Why are lawyers targeted?
- What are some examples of scams against lawyers?
  - Business Email Compromise (BEC) and Business Identity Compromise (BIC)
  - Check and trust account fraud
  - AI, deepfake and technology-enabled threats
- Where do controls fail?
- What are some ethical duties related to scams?
- What are some best practices to combat scams?
- Q&A

SCAM TYPOLOGIES AND THEIR SIGNIFICANCE FOR LEGAL PROFESSIONALS

LEARNING OBJECTIVES

- ✓ Define a scam and understand why it matters for lawyers
- ✓ Examine the modern scam landscape and explore why legal professionals are targeted differently from general public
- ✓ Analyze common scam typologies affecting law firms
- ✓ Understand ethical duties under the American Bar Association (ABA) Model Rules and professional liability exposure
- ✓ Highlight best practices for prevention and response

WHAT IS A SCAM?

An intentional deception that induces the victim to authorize a transaction, disclose information, or grant access

- In many scam scenarios, the lawyer initiates the transfer or disclosure;
- Authorization > scam vs. Unauthorized > fraud
- The authorization may be based on false information;
- It is still **an authorized act** that may lead to serious implications to ethical responsibility and insurance coverage;
- Even when an attorney is deceived, the resulting actions may still be treated as authorized under the law;
- This explains why scam prevention is not just an IT concern but a core professional responsibility.

INTERACTIVE HYPOTHETICAL # 1

Imagine you receive an email from a long-standing corporate client instructing you to wire settlement funds to a new account due to “internal restructuring.” The email appears consistent with prior communications and references a legitimate matter. You authorize the transfer. Two days later, the client reports the funds never arrived.

Pause for a moment and consider: was this transaction authorized? And if so, how might that affect insurance coverage and ethical analysis?

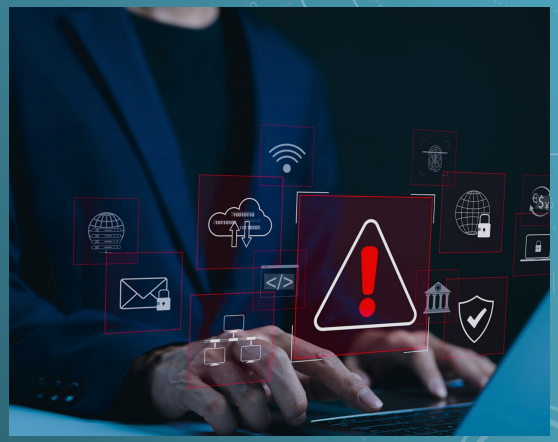
WHAT IS THE MODERN SCAM LANDSCAPE?

- Technologically advanced
- Psychologically sophisticated
- Highly scalable
- Run by organized, transnational networks
- Function like businesses, with specialization and automation
- Examples:
    - Phishing emails
    - Spoofed phone numbers
    - Malware
    - Ransomware

WHY ARE LAWYERS TARGETED?

Lawyers' uniquely valuable position:

- Manage client funds
- Control trust accounts
- Possess confidential and privileged information
- Coordinate high-value transactions
- A single compromised attorney or firm yield immediate rewards
- Legal practice involves predictable and time-sensitive workflows
- Scammers study workflow processes, making deception more difficult to detect
- Unlike mass consumer scams, the ones targeting lawyers are highly tailored and specific



INTERACTIVE HYPOTHETICAL # 2

Consider a small firm handling multiple real estate closings each week. A scammer gains access to one attorney's email account and quietly monitors transactions.

Ask yourself: how many matters could be affected before the breach is detected, and how many clients could be harmed by a single compromised account?

AUTHORITY AND HIERARCHY EXPLOITATION

Vulnerabilities:

- ✓ Hierarchical structures within law firms
  - Managing partners, senior attorneys, general counsel
- ✓ Court systems
  - Judges and court officials
- ✓ Urgency and authority of communication
  - Creates pressure to comply quickly
- ✓ Junior attorneys and staff may hesitate to question requests
  - Especially when confidentiality is emphasized

INTERACTIVE HYPOTHETICAL # 3

Imagine you receive an email that fits perfectly into an existing thread with opposing counsel or the court. The tone, signature, and timing all seem right.

Ask yourself honestly: at what point would you stop to verify the message, and what verification step would you take?

BUSINESS EMAIL COMPROMISE (BEC) AND BUSINESS IDENTITY COMPROMISE

- BEC is a sophisticated cybercrime where attackers impersonate trusted parties via email or voice to manipulate business transactions and redirect funds to fraudulent accounts
- BIC involves criminals stealing a company's identity to commit fraud, often through sophisticated email scams like BEC, where attackers impersonate executives or vendors to trick employees into transferring funds or revealing sensitive data, leading to significant financial losses
- Among the top financial cybercrime threats
- 21,442 complaints and $2.77B in total reported BEC losses across all sectors (FBI Internet Crime Complaint Center - IC3, 2024)

INTERACTIVE HYPOTHETICAL # 4

A managing partner emails, texts or calls accounting staff stating, “I’m boarding a flight. Please send the wire now. I’ll explain later.”

Would your firm’s policies allow that transfer to proceed? If so, what risk does that create?

ANATOMY OF A BEC ATTACK

1 Step **Reconnaissance**

Attackers research targets, gathering information about real estate deals, key personnel, and transaction timelines from public sources and social media.

2 Step **Phishing**

Cybercriminals craft convincing emails to trick victims into revealing login credentials for email accounts or transaction systems.

3 Step **Account Compromise**

Once credentials are obtained, attackers access legitimate accounts or create lookalike addresses with subtle differences (e.g., changing .com to .net).

4 Step **Social Engineering**

Using insider knowledge and terminology, attackers create urgent messages to manipulate recipients into changing wire instructions or payment details.

5 Step **Fund Diversion**

Funds are transferred to attacker-controlled accounts, often through multiple international hops to complicate recovery efforts.

CHECK AND TRUST ACCOUNT FRAUD

- Counterfeit checks presented at settlement payments
- Retainers from clients
- When the check bounces, the trust account may become deficient
- Even if a lawyer is deceived, violation of trust-account rules may be claimed

TECHNOLOGY-ENABLED THREATS

- Malware, remote access trojans, SIM swamping, credential stuffing, botnets allow criminals to compromise computer systems and intercept communications
- Once inside a firm's network, scammers may quietly monitor activity before acting
- AI has dramatically escalated scam risks
- Voice cloning can replicate a client's or partner's voice
- Deepfake video can impersonate
- AI-generated text mimics the style and vocabulary

INTERACTIVE HYPOTHETICAL # 5

You receive a voicemail that sounds exactly like your client, urgently asking you to release funds. There is no email follow-up.

Would you treat that call as sufficient authorization? What verification step would you require?

WHERE DO CONTROLS FAIL?

- Lack of regular training
- Absence of written policies and procedures
- Wiring changes accepted via email
- No voice verification protocol (no dual control callbacks)
- Inadequate domain and mailbox protection
- Weak or no multi-factor authentication (MFA)
- Clients unaware of BEC risks
- No verification of parties involved in the transaction
- Insider risk

INTERACTIVE HYPOTHETICAL # 6

A paralegal processes a fraudulent wire instruction after receiving a convincing email.

Ask yourself: under the Model Rules, who bears responsibility, and what supervisory steps might regulators expect to have been in place?

WHAT ARE SOME ETHICAL DUTIES RELATED TO SCAMS?

- American Bar Association (ABA) Model Rules
  - Model Rule 1.1 requires technological competence
  - Rule 1.15 requires safeguarding client funds
  - Rule 1.6 requires safeguarding confidentiality, including electronic data
  - Rule 5.3 requires supervision of staff

INTERNAL CONTROLS THAT WORK

- People:
  - Mandatory BEC/wire-fraud training for every party touching funds (agents, escrow/title staff, attorneys)
  - Live phishing and mailbox-rule simulations
  - Exercises for the first 24 hours of response (SWIFT recall/hold, IC3 complaint, FinCEN Rapid Response, law enforcement)
- Process:
  - Verification of every wire by verified phone, not email
  - Dual control (voice-verified) for wiring changes (never to the number in the email requesting the change)
  - Signed standard “safe-wiring” disclosures to buyers/sellers
  - Tight vendor onboarding for payoff lenders, attorneys, title agents
- Technology:
  - Secure portals, multi-factor authentication, domain protections
  - Encrypted messaging for wire instructions and payoff letters

INTERACTIVE HYPOTHETICAL # 7

If your firm required a mandatory call-back to a known number for all wire instructions, how many of the hypotheticals we've discussed today would have been stopped before harm occurred?

INCIDENT RESPONSE PLAN

- Containment
- Reset password immediately following hack suspicion
- Evidence preservation
- Client notification
- Coordination with financial institutions
- File a complaint at FBI IC3 unit www.ic3.gov within 24 hours

EXPERT CA PROVIDES:

- ✓ Training on white-collar crime prevention and forensic expert witness services

- ✓ Investigation:
  - Forensic Accounting,
  - Digital Forensics,
  - Private Investigation,
  - Witness Interview, Evidence Gathering and Analysis

- ✓ Expert Witness & Litigation Consulting

Thank you.

Questions?

Expert CA
© 2022-2026 All Rights Reserved

HOW SCAMS OCCUR

Scams are no longer simply awkward emails from distant princes asking for your bank details. They are now highly sophisticated operations run by individuals and organized groups who leverage technology, psychology and timing to exploit their victims. To protect yourself and others, it's crucial to understand how scams occur – how they start, how they manipulate and how they succeed.

THE SETUP: TARGETING THE VICTIM

Criminals often begin by identifying potential targets. This can happen in various ways:

- **Random targeting:** Mass emails, robocalls and text messages are sent out in bulk, hoping someone will bite.
- **Selective targeting:** Criminals use data breaches, social media or public records to zero in on specific individuals who are the most likely to respond, such as the elderly, job seekers or those looking to invest.
- **Phishing and social engineering:** Criminals may gather information from public profiles to personalize the scam, increasing its credibility.

During this phase, criminals' goals are to establish contact and build a foundation for manipulation.

BUILDING TRUST

Once the initial contact is made, criminals use psychological techniques to weaken their potential victim's defenses.

- **Emotional pleas:** Romance scams generate a sense of affection and companionship. Charity scams tug on your heartstrings. Investment scams excite you with visions of wealth.
- **Fear and urgency:** Threatening calls from "government officials," fake tech support people claiming your computer is infected, or bogus messages from your bank demanding immediate action are designed to quickly induce fear and panic.
- **Authority impersonation:** To gain credibility, many criminals pose as trusted individuals, such as public figures, employers, friends or relatives.

The goal is always to exploit basic human emotional responses: trust, fear, greed and love.

HOW SCAMS OCCUR

THE HOOK: ASKING FOR SOMETHING

Once criminals have built enough trust or fear, they make a request. This is the critical point where the scam turns into theft.

- **Money:** Traditional money transfers, cryptocurrency, gift cards or donations.
- **Information:** Personal details, passwords, bank account numbers or Social Security numbers.
- **Access:** Granting remote access to your computer, installing malicious apps or clicking on infected links.

The initial "ask" is often small, just enough to test the waters before scaling up to larger requests.

THE EXIT: VANISHING ACT

Once criminals get what they want, they disappear:

- Phone numbers go dead.
- Email addresses bounce back.
- Websites vanish or become inactive.
- Social media profiles are deleted or blocked.

Often, victims don't even realize they've been scammed until much later – when a package never arrives, money is gone or identity theft surfaces.

REPETITION OR RETARGETING

Some criminals don't stop after one incident. They may:

- Re-target the same victim, pretending to be someone else (e.g., offering "recovery" services for the initial scam).
- Sell victims' information on the dark web, leading to more scams down the line.
- Use successful scams as templates, refining their tactics and updating them for different platforms or regions.

HOW SCAMS OCCUR

COMMON CHANNELS USED BY CRIMINALS

- Phone calls (vishing)
- Text messages (smishing)
- Emails (phishing)
- Social media messages
- Fake websites or pop-ups
- Online marketplaces or dating apps

No matter the medium, the method remains the same: contact, build trust or fear, extract value and disappear.

Scams happen because they work. They exploit our human vulnerabilities. Knowledge continues to be your best defense. By understanding the methods criminals use, you can identify the red flags, better resist manipulation and help stop the cycle of scams.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

WHY YOU SHOULD CARE ABOUT SCAMS

Scams have been around for thousands of years. However, they have become increasingly sophisticated in recent years, resulting in billions of dollars of losses. Romance scams, investment scams, fake job offers and other scams impact millions of people annually worldwide. Many believe this can't happen to them, despite prevalent news reports, ongoing education and awareness efforts. Whether you believe you will fall victim or not, it is important to be aware of what is happening.

Scams don't discriminate. The criminals target young professionals, retirees, students, kids, business owners – in other words, everyone. No one is immune. Victims span all demographics, regardless of age, income level or education, as shown in reports from the Federal Trade Commission (FTC) and other sources. Criminals prey on trust, fear, urgency and hope – emotions that are experienced by everyone. Even if you have not yet been a target, you likely know someone who has.

The financial cost of scams is overwhelming. Globally, scams cost individuals and businesses billions of dollars each year. We are seeing the same trends domestically. The data reported likely reflects only a fraction of the losses, as not all victims report the scams. Many victims are too embarrassed to come forward, resulting in significantly understated data.

Scams fuel organized crime. The money stolen through scams may fund organized crime and other illicit activities, such as money laundering and human trafficking. Stopping scams is about more than protecting yourself – it's about cutting off a very profitable revenue stream for sophisticated fraud rings.

Scams take an emotional and psychological toll. The impacts of scams are not just about losing money. Victims often suffer from shame, anger and a deep sense of betrayal (especially in romance or impersonation scams). These emotional wounds can linger, leading to mental health issues and loss of trust in others. The psychological fallout may even discourage victims from seeking help or reporting future incidents.

Scams undermine society and institutions. When scams occur, they can destroy trust in the internet, the financial system, financial institutions and in each other. Scam victims may lose their sense of safety. For example, seniors may become afraid to answer the phone, small businesses may lose confidence in online transactions, and misinformation campaigns may further impact consumers and businesses.

WHY YOU SHOULD CARE ABOUT SCAMS

Knowledge is power. Caring about scams means staying aware and informed — and helping others do the same. Scams flourish in silence and ignorance. When people learn how scams work and share that knowledge, it makes the job much harder for criminals. Simple habits, such as verifying emails, questioning urgent requests, checking website addresses and having open conversations about online safety, can significantly reduce your risk.

You can be a line of defense. Even if you have never been scammed, you can learn enough to help protect those around you. Elderly relatives, young teens or less tech-savvy friends may not recognize red flags. Being more aware allows you to identify potential threats, offer guidance and report suspicious activity.

Scams don't discriminate. They threaten individual well-being, economic stability and public trust. Awareness about scams means you are informed, proactive and prepared. The next time someone shares a too-good-to-be-true offer or a suspicious link lands in your inbox, don't just ignore it. Think critically. Ask questions. Educate others. The more cognizant we are, the harder it becomes for criminals to succeed.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.