PROGRAM MATERIALS
Program #3616
February 3, 2026

Synthetic Identity Fraud and Its Challenge for Legal Professionals

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

Celesq® AttorneysEd Center
www.celesq.com

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

Expert CA

Synthetic Identity Fraud and Its Challenge for Legal Professionals

- Live Webcast CLE Presentation | Celesq AttorneysED Center | February 3, 2026
- Prepared by Alex Kulikov, MS, CFCI, CFCS, GAAP, PMP

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

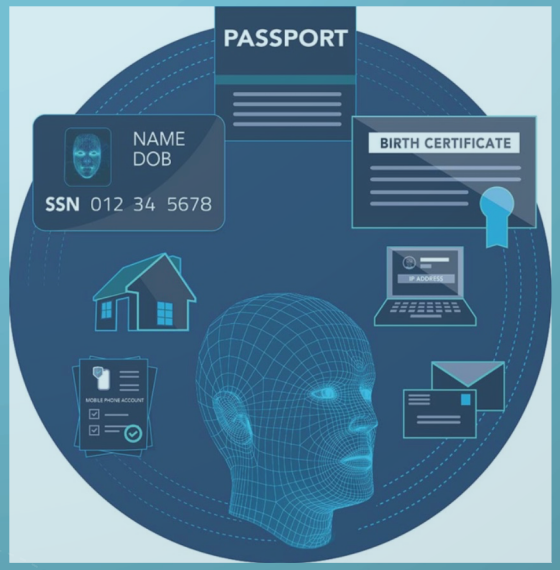
CONFLICT-OF-INTEREST DISCLOSURE & LEGAL DISCLAIMER

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

SYNTHETIC IDENTITY FRAUD AND ITS CHALLENGE FOR LEGAL PROFESSIONALS



- What are the learning objectives?
- What is synthetic identity fraud?
- Why are legal professionals high-risk targets?
- What is the regulatory framework?
- What are some key legal and enforcement trends?
- What are law firm operational vulnerabilities?
- What are best practices for legal professionals?
- What are incident response and legal exposure?
- What are some anticipated trends?
- Q&A

LEARNING OBJECTIVES

- ✓ Define synthetic identity fraud and distinguish it from traditional identity theft
- ✓ Identify how synthetic identity fraud affects legal practice areas
- ✓ Understand regulatory and ethical obligations impacting lawyers
- ✓ Recognize litigation, disciplinary, and liability risks
- ✓ Apply practical safeguards and response strategies

WHAT IS SYNTHETIC IDENTITY FRAUD?

- Combination of real and fabricated identifiers
  - Real Social Security numbers with false names, addresses, records
- No single identifiable victim
  - No individual sees immediate harm
- Long-term cultivation of legitimacy
  - Detection is delayed

WHAT ARE LEGAL PROFESSIONALS HIGH-RISK TARGETS?

- Client intake and trust obligations
- Access to escrow and settlement funds
- Authority to move money and execute documents
- Ethical duty of confidentiality
- Digital onboarding and remote transactions
- Use of automated verification systems
- Frauds targeting lawyers are highly tailored and specific
- Legal practice involves predictable and time-sensitive workflows
- Hierarchical structures within law firms

INTERACTIVE HYPOTHETICAL # 1

Imagine you receive a request from a new corporate client seeking entity formation and escrow services. All documents verify successfully, but months later the entity is linked to fraud.

What verification steps should counsel have taken beyond document review?

WHAT IS THE REGULATORY FRAMEWORK?

Primary Regimes Affecting Legal Professionals:

- ✓ Anti-money laundering (AML)
  - Bank Secrecy Act principles (indirect application)
- ✓ Data privacy and security laws
  - Gramm-Leach-Bliley Act (GLBA)
- ✓ Consumer protection statutes
  - FTC Safeguards Rule (where applicable)
- ✓ Professional conduct rules
  - Bar rules on competence and supervision

KEY LEGAL AND ENFORCEMENT TRENDS

- Negligence claims against intermediaries
- Regulatory expectations of proactive detection
- Heightened scrutiny of trust account practices
- Ethical duties implicated
  - Duty of competence (technology literacy)
  - Duty of confidentiality
  - Duty to supervise staff and vendors
  - Fiduciary responsibility

ETHICAL DUTIES RELATED TO SYNTHETIC IDENTITY FRAUD?

- 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

INTERACTIVE HYPOTHETICAL # 2

Consider receiving wiring instructions changes mid-transaction. Instructions are provided by the recently engaged client with a synthetic identity. Funds are lost.

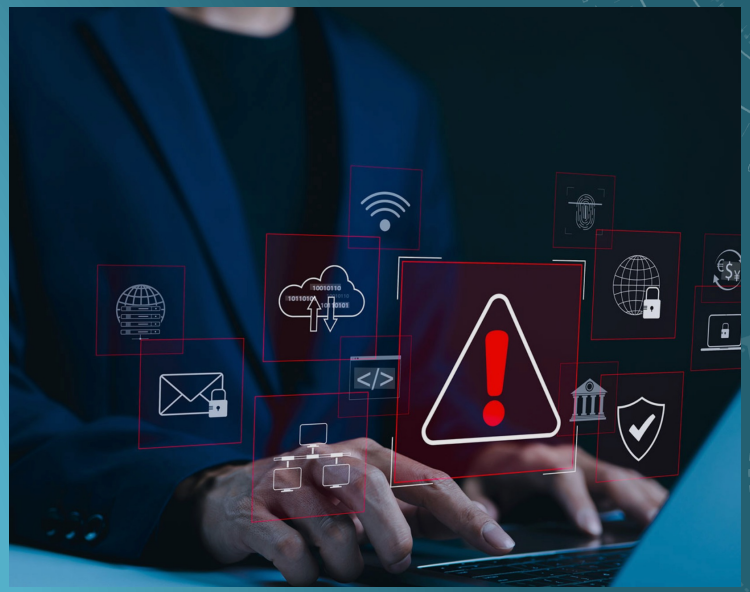
Ask yourself: is this malpractice, and ethical breach, or both?

WHAT ARE LAW FIRM OPERATIONAL VULNERABILITIES?

- Workflows designed for efficiency, not risk resilience
- Remote work
- Virtual notarization
- Reliance on vendors for identity verification, payment processors
- Electronic signatures
- Cloud-based document management
- Digital client portals and client engagement
- Absence of written training procedures
- Limited staff training

BEST PRACTICES FOR LEGAL PROFESSIONALS

- Risk-based approach
- Integrate governance and technology
- Formal written policies and response plan
- Multiple controls at various stages
- Layered identity verification
- Vendor due diligence
- Analyzing client's profile
- Periodic reassessment
- Mandatory callback and verification
- Segregation of duties
- Multi-factor authentication



INTERACTIVE HYPOTHETICAL # 3

Imagine you receive a request from a newly formed entity seeking to engage in a complex, high-value transaction with compressed timelines.

Shouldn't the legal team evaluate whether the proposed transaction aligns with the client's stated background, business purpose, and financial profile, even if the formation documents appear valid?

INCIDENT RESPONSE AND LEGAL EXPOSURE

- Written incident response plan
- Follow communication protocols
- Documented responses
- Immediate containment
- Evidence preservation
- Client notification
- Regulatory assessment
- Coordination with financial institutions
- File a complaint at FBI IC3 unit www.ic3.gov within 24 hours

WHAT ARE SOME ANTICIPATED TRENDS?

- AI has dramatically escalated fraud risks
- AI-generated synthetic personas
- Voice cloning can replicate a client's or partner's voice
- Deepfake video can impersonate
- Regulatory expansion to legal professionals
- Increased disciplinary actions

KEY TAKEWAYS

- Synthetic identity fraud is a professional responsibility issue
- Legal professionals are gatekeepers, not bystanders
- Prevention is a legal defense strategy
- Regular training and firm-wide commitment to stop synthetic identity fraud
- Written policies defining internal controls are critical

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:

SYNTHETIC IDENTITY FRAUD WEBINAR – CLE SUBMISSION PACKET

Prepared for: Celesq, AttorneysED Center

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

Date: January 20, 2026

PROGRAM TITLE

Synthetic Identity Fraud and Its Challenge for Legal Professionals

PROGRAM DESCRIPTION

Legal professionals are increasingly challenged by synthetic identity fraud that exploits trust, authority structures, predictable workflows, and the unique responsibilities lawyers hold over confidential information and client funds. This Continuing Legal Education (CLE) program examines the growing threat of synthetic identity fraud and its impact on legal professionals.

Participants will explore how synthetic identities are created, why lawyers are uniquely vulnerable, and how ethical duties, regulatory expectations, and emerging case law shape professional responsibility. The course provides practical risk mitigation strategies and interactive hypotheticals applicable across practice areas.

LEARNING OBJECTIVES

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

1. Define synthetic identity fraud and distinguish it from traditional identity theft
2. Identify how synthetic identity fraud affects legal practice areas
3. Understand regulatory and ethical obligations impacting lawyers
4. Recognize litigation, disciplinary, and liability risks
5. Apply practical safeguards and response strategies

TIMED AGENDA (60-Minute CLE Program)

00:00 - 5:00 - Introduction and Overview

- Learning objectives
- Rise of global scam operations
- Legal professionals are high-risk targets

5:00 - 10:00 - Defining Synthetic Identity Fraud

- Difference between identity theft and synthetic identity fraud
- Entirely fictitious identity, no single victim
- Legal professionals may be serving clients that never existed

10:00 - 20:00 - Regulatory Framework

- Federal Trade Commission
- Bank Secrecy Act and FinCEN
- Gramm-Leach-Bliley Act
- American Bar Association Model Rules

20:00 - 30:00 - Key Legal Enforcement Trends

- Reasonable verification
- Negligence claims against legal professionals
- Synthetic identity fraud as a foreseeable operational risk

30:00 - 40:00 - Ethical Duties

- Model Rule 1.1
- Model Rule 1.15
- Model Rule 1.6
- Model Rule 5.3

40:00 - 45:00 - What Are Law Firms' Operational Vulnerabilities?

- Workflows
- Remote work
- Virtual onboarding
- Electronic signatures
- Cloud-based document management
- Third-party vendors

45:00 - 50:00 - Best Practices And Strategic Responses

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

50:00 - 57:00 - Anticipated Trends

- Escalated fraud risks
- AI-generated deepfake video and audio
- Regulatory scrutiny

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:

- Synthetic Identity Fraud CLE Submission Handout (35 pages, double-spaced)
- References to Statutes, Rules and Regulations, Cases and Reports
- 20-Page Synthetic Identity Fraud Presentation Slide Deck, including Interactive Hypotheticals
- The Federal Reserve Toolkit - Allure of a Synthetic to a Fraudster: Ease of Creation

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

www.expertadvisors.us (707)330-0054

CLE Presentation: Synthetic Identity Fraud and Its Challenge for Legal Professionals

Submission Handout

Table of Contents

I. Introduction

Synthetic identity fraud has emerged as one of the fastest-growing and most complex forms of financial and identity-based crime. Unlike traditional identity theft, which relies on the misuse of an existing individual's complete personal data, synthetic identity fraud involves the deliberate construction of a partially or entirely fictitious identity. These identities are often created by blending real data points- such as a valid Social Security number, national identification number, or tax identifier, with fabricated names, addresses, dates of birth, or digital footprints. Over time, fraudsters nurture these synthetic identities to appear legitimate, allowing them to bypass identity verification systems, establish credit histories, engage in transactions, and eventually perpetrate large-scale financial fraud.

For legal professionals, synthetic identity fraud presents a uniquely challenging risk profile. Law firms, corporate legal departments, compliance teams, and transactional lawyers increasingly operate in environments that rely on digital onboarding, remote client engagement, and third-party verification systems. At the same time, legal professionals carry fiduciary duties, confidentiality obligations, and regulatory responsibilities that heighten both exposure and liability when fraud infiltrates legal workflows. The convergence of technology, regulation, and professional responsibility places lawyers at the center of the fight against synthetic identity fraud, whether they are advising clients, conducting due diligence, managing trust accounts, or defending organizations after a breach or fraud event.

This presentation provides a basic examination of synthetic identity fraud, its operational mechanics, its legal and regulatory implications, and its specific impact on legal professionals. It analyzes the regulatory landscape, explores key cases that illustrate emerging risks, and offers an

expert's proposed framework for how legal professionals can adapt policies, processes, and professional practices to mitigate both legal and reputational harm.

II. Understanding Synthetic Identity Fraud

Synthetic identity fraud differs fundamentally from traditional identity theft in both execution and detectability. In classic identity theft, a victim typically becomes aware of misuse through unauthorized transactions or credit activity. In contrast, synthetic identities may not have a direct human victim who recognizes the fraud, making detection slower and recovery more complex. Fraudsters frequently exploit unused or newly issued government identifiers, such as those belonging to minors, deceased individuals, or individuals with limited credit histories, combining them with invented biographical data.

Once created, a synthetic identity is often "growing" over months or years. Fraudsters may open small accounts, apply for low-risk services, or interact with digital platforms to build a credible profile and credit history. Eventually, these identities are used to obtain substantial credit, execute fraudulent contracts, launder money, or facilitate other crimes. For legal professionals, this creates a paradox: the more legitimate a synthetic identity appears, the more likely it is to pass standard legal and compliance checks.

Advancements in data aggregation, artificial intelligence (AI), and remote identity verification have further complicated the landscape. Automated systems designed to streamline onboarding can inadvertently increase fraud risk when synthetic identities are optimized to exploit verification thresholds. Legal professionals who rely on third-party verification services

may assume compliance without fully understanding the limitations of these systems, increasing institutional exposure.

III. Why Legal Professionals Are Particularly Vulnerable

Legal professionals occupy a uniquely trusted and powerful position within financial, corporate, and personal transactions, a role that makes them especially vulnerable to synthetic identity fraud. Unlike many other professional service providers, lawyers function as both advisors and gatekeepers. Their involvement often confers legitimacy on clients, entities, and transactions that may otherwise receive heightened scrutiny from financial institutions, courts, or regulators. Law firms routinely handle highly sensitive personal and financial information, control client trust and escrow accounts, facilitate mergers and acquisitions, manage real estate closings, oversee estate planning and probate matters, and administer litigation settlements. Each of these functions creates multiple points at which a synthetic identity can be introduced, relied upon, and ultimately weaponized against the firm and its clients.

Client intake and onboarding processes represent one of the most significant points of law firms' exposure. Attorneys are ethically obligated to identify and verify their clients, a duty that has grown more complex as legal practice has shifted toward remote engagement, electronic signatures, and digital document exchange. While lawyers in the United States are not uniformly subject to the same customer identification program requirements imposed on financial institutions, they nonetheless operate under overlapping compliance expectations arising from anti-money laundering frameworks, professional conduct rules, and federal enforcement priorities. The Bank Secrecy Act (BSA) and its implementing regulations, administered by the

Financial Crimes Enforcement Network (FinCEN), establish national expectations for customer due diligence and beneficial ownership transparency, particularly in high-risk transactions such as real estate, entity formation, and financial structuring.[1] In addition, the Corporate Transparency Act (CTA) now requires disclosure of beneficial ownership information for many U.S. entities, increasing the risk that lawyers who assist in entity formation or governance may unknowingly rely on synthetic identities embedded within ownership structures.[2]

Synthetic identities that successfully pass superficial or document-only verification can enable fraudsters to retain counsel, establish attorney-client relationships, and gain access to protected firm systems, confidential information, and transactional authority. Once representation begins, disengaging from a fraudulent client becomes legally and ethically complex. Lawyers must balance duties of confidentiality and loyalty under professional conduct rules with obligations to avoid assisting fraudulent or criminal conduct. In practice, this can leave firms stuck in matters involving fabricated individuals or entities, with heightened exposure to claims that they failed to conduct reasonable due diligence or ignored red flags during client intake. Courts and regulators increasingly evaluate whether lawyers exercised reasonable professional judgment rather than merely relying on automated verification tools.

---

[1] 31 U.S.C. §§ 5311 - 5336; 31 C.F.R. Chapter X, Bank Secrecy Act and FinCEN regulations. https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X

[2] 31 U.S.C. § 5336 Corporate Transparency Act, (beneficial ownership information reporting requirements). March 2025, FinCEN issued an interim rule exempting U.S. domestic reporting companies from filing, citing ongoing legal uncertainty and to support small businesses, focusing future efforts on foreign entities. The CTA remains law, but FinCEN is not enforcing it against U.S. domestic companies; however, legal challenges persist, and enforcement could theoretically be reinstated. While CTA has faced intense pushback, leading to legal uncertainty, March 2025 rule change has effectively paused domestic reporting requirements, making the controversy less about immediate compliance and more about the future scope of the law and its constitutional validity. https://www.law.cornell.edu/uscode/text/31/5336

Trust accounts and escrow services present an even higher-risk environment. Attorneys who manage client funds act as fiduciaries, and misuse of those funds- whether intentional or not, can trigger severe consequences. Synthetic identities may be used to establish shell companies, impersonate beneficiaries, or submit fraudulent instructions for the disbursement of settlement proceeds or purchase funds. For example, a fraudster using a synthetic identity may appear as a legitimate corporate officer or estate beneficiary, request a last-minute change to wiring instructions, and divert funds before the fraud is detected. When losses occur, legal professionals may face allegations of negligence, breach of fiduciary duty, failure to supervise staff, or violations of trust account rules. American Bar Association (ABA) Model Rules and courts have consistently treated trust account mismanagement as one of the most serious forms of professional misconduct, regardless of whether the lawyer personally benefited from the loss.[3] The growing number of wire fraud and synthetic identity schemes has led regulators and malpractice insurers to scrutinize whether law firms implemented reasonable safeguards, such as independent verification of payment instructions and segregation of duties, rather than relying solely on client representations.

Litigation and dispute resolution processes also present growing risks. Synthetic identities may be used to file fraudulent claims, fabricate plaintiffs or defendants, or manipulate mass arbitration or class action filings. In some cases, synthetic claimants have been used to inflate damages, manufacture standing, or extract nuisance settlements. As courts have expanded

[3] 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/

the use of electronic filing systems, remote hearings, and virtual appearances, traditional face-to-face identity verification safeguards have diminished. Federal and state courts increasingly rely on attorneys' certifications and representations regarding the identity and authority of the parties they represent. Under rules such as Federal Rule of Civil Procedure 11, lawyers have an affirmative obligation to ensure that filings are not presented for improper purposes and that factual contentions have evidentiary support.[4] When a synthetic identity is later uncovered in litigation, attorneys may face sanctions, disqualification, or reputational harm if it appears they failed to conduct reasonable inquiry into their client's identity or claims.

Taken together, these factors place legal professionals in a position of heightened vulnerability. Synthetic identity fraud exploits the trust placed in lawyers, the complexity of modern legal practice, and the potential conflict between efficiency and due diligence. As regulatory expectations evolve and courts increasingly scrutinize the role of professional legal advisors, lawyers can no longer assume that identity verification is just a simple administrative task. Instead, it is becoming a core component of professional responsibility, risk management, and compliance within the legal profession.

IV. Regulatory and Compliance Landscape

Synthetic identity fraud sits at the intersection of multiple regulations because it is simultaneously a financial crime risk, a privacy and data-security risk, and a professional responsibility risk. For legal professionals, the compliance challenge is rarely limited to one statute or one regulator. Instead, synthetic identity schemes tend to exploit the seams between

[4] Federal Rules of Civil Procedure 11(b) (requiring reasonable inquiry and factual support for pleadings and representations to the court). https://www.law.cornell.edu/rules/frcp/rule_11

regulations: a “client” who is not who they claim to be, a corporate entity formed with concealed beneficial ownership, a remote onboarding process that over-relies on document checks, and a transaction that results in unauthorized funds movement or a data exposure event. When that happens, the legal team’s exposure can range from consumer-protection enforcement, financial-crime expectations, privacy safeguards, breach-notification duties, malpractice theories, trust-account rules, and professional discipline- often at the same time.

In the United States, the Federal Trade Commission (FTC) serves as a central enforcement and standard-setting body for identity theft and consumer protection in contexts that are directly relevant to many law firms, particularly those that handle personal data, interact with consumer financial products, or advise clients on fraud prevention programs. The FTC’s general authority to police “unfair or deceptive acts or practices” under Section 5 of the FTC Act frequently includes enforcement actions involving weak identity verification controls, misleading privacy practices, or inadequate data-security measures that enable identity-related harms.[5] When synthetic identity fraud is facilitated by weak data governance- such as weak access controls to client intake records or insufficient vendor security, law firms that fall within the FTC’s jurisdictional scope (or that advise clients subject to FTC enforcement) must treat identity verification and data protection as linked compliance problems, not separate operational issues.

FTC-linked compliance obligations can also arise from sector-specific identity theft rules that may be triggered by certain kinds of legal practices. For example, the “Red Flags Rule” under the Fair and Accurate Credit Transactions Act amendments to the Fair Credit Reporting

[5] Federal Trade Commission Act, 15 U.S.C. § 45(a) (prohibiting unfair or deceptive acts or practices). https://www.law.cornell.edu/uscode/text/15/45

Act, can apply to organizations that qualify as "creditors" and maintain "covered accounts."[6] While many law firms will not be creditors, some firms do extend payment plans or otherwise meet thresholds in certain contexts. Even when the rule does not apply directly, it has become a benchmark for what regulators and plaintiffs' experts describe as "reasonable" identity theft prevention controls. In practice, the same types of controls emphasized by Red Flags-style frameworks- risk-based detection, escalation procedures, and documented response, are precisely the controls that reduce exposure when synthetic identity fraud later becomes a litigation or insurance dispute.

At the financial crime level, the most important national framework is the Bank Secrecy Act (BSA) and its implementing regulations, administered by the Department of the Treasury (DOT) through the FinCEN.[7] The BSA's core provisions are aimed at financial institutions, but it increasingly influences legal practice because lawyers are frequently involved in the types of transactions that the BSA seeks to protect from abuse: beneficial ownership concealment, laundering through corporate structures, high-value real estate purchases, and movement of funds through intermediaries.

A common synthetic identity pattern illustrates how a law firm may fall under the BSA framework. A fraudster creates a synthetic identity, uses it to register a shell company, and then uses that entity to open accounts, retain counsel, or appear as a principal in a transaction. If lawyers facilitate entity formation, escrow arrangements, or property transactions without

---

[6] 15 U.S. Code § 1681m - Requirements on users of consumer reports (e) Red flag guidelines and regulations required https://www.law.cornell.edu/uscode/text/15/1681m

16 C.F.R. § 681.1 (identity theft prevention programs - "Red Flags Rule"). https://www.law.cornell.edu/cfr/text/16/681.1

[7] 31 U.S.C. §§ 5311 - 5336; 31 C.F.R. Chapter X

adequate scrutiny of identity, the firm may not be directly liable under the BSA the way a bank is, but it can draw attention of post-incident inquiries into gatekeeper diligence and the reasonableness of controls- especially if the transaction involves a bank's suspicious activity monitoring or law enforcement investigation.

A major development that has elevated beneficial ownership verification as a compliance issue for lawyers is the Corporate Transparency Act, which requires many corporations, LLCs, and similar entities to report beneficial ownership information to FinCEN.[8] Synthetic identities can be used to populate the beneficial ownership record, either by presenting fabricated "beneficial owners" or by hiding real owners behind synthetic nominees. Law firms that assist with entity formation, governance, transactional diligence, or regulatory compliance must now treat beneficial ownership as a fraud-risk control point.

A real-world example is the use of synthetic "managing members" to give an entity a governance structure during onboarding, only for the entity to later serve as a vehicle for diverting escrow funds or engaging in contract fraud. The legal risk to the firm is not only that the transaction fails, but that the firm's file reflects weak verification of who had authority to act, who controlled the entity, and whether the firm took reasonable steps to understand ownership and purpose.

Privacy and information security obligations add another layer. The Gramm-Leach-Bliley Act (GLBA) requires "financial institutions" to protect the security and confidentiality of customer information and to implement safeguards for nonpublic personal information.[9]

---

[8] *Ibid.*

[9] 15 U.S.C. §§6801-6809, Gramm-Leach-Bliley Act (privacy and safeguards provisions). https://www.notarylearningcenter.com/pdf/GrammLeachBliley.pdf

While many law firms are not themselves "financial institutions," the GLBA ecosystem matters to legal professionals in at least three recurring ways. First, firms that provide services to financial institutions often handle GLBA-covered information as service providers, pulling them into contractual safeguard requirements, vendor management obligations, and incident response expectations shaped by GLBA compliance programs. Second, some law firms have practice lines- such as consumer financial services work, debt collection-related representation, or advisory services tightly integrated into financial products, where the firm's data practices may be scrutinized against GLBA-driven standards. Third, even outside direct GLBA applicability, the FTC's Safeguards Rule (issued under GLBA authority) has become a widely referenced measure for "reasonable" information security, emphasizing written security programs, risk assessments, access controls, encryption, and vendor oversight.[10] Synthetic identity fraud thrives on weak controls around the collection, storage, and verification of personal identifiers. As a result, information security and identity verification become inseparable from a compliance standpoint.

Privacy and breach-notification regulations further complicate the picture because synthetic identity fraud incidents often involve data access or disclosure. In practical terms, a synthetic identity event may begin as "just" an intake fraud but then later become a reportable security incident if the fraudster gains access to client portals, document management systems, or payment platforms. Although there is no single, comprehensive federal privacy statute of general applicability, there are federal sectoral regimes that can be triggered depending on the firm's

[10] 16 C.F.R. pt. 314 (FTC Safeguards Rule under GLBA authority). https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf

clients and data. For example, if a law firm acts as a business associate to covered entities in healthcare contexts, Health Insurance Portability and Accountability Act (HIPAA)'s privacy and security rules and breach notification requirements may become directly relevant to the firm's incident response posture.[11]

In consumer reporting contexts, the Fair Credit Reporting Act and related provisions can shape how identity verification data is obtained and used, and how adverse actions are handled by clients advised by the firm.[12] When synthetic identity fraud causes a data breach, firms must coordinate rapid legal analysis across applicable state breach laws, contractual notification clauses, insurance requirements, and professional conduct duties, all while preserving privilege and ensuring accurate communications that avoid admissions not supported by investigation.

A few words about international regulations. The European Union's General Data Protection Regulation (GDPR) has significant implications for global law firms and cross-border transactions because fraud prevention requires the processing of personal data and often involving sensitive information. Synthetic identity fraud detection programs can pressure organizations to collect more data, retain it longer, and share it more broadly with vendors- all of which can conflict with GDPR principles such as data minimization, purpose limitation, storage limitation, and lawful processing.[13] A common compliance pitfall is "over-collection" justified by fraud prevention: firms may gather expansive identity datasets during onboarding or due

---

[11] 42 U.S.C. § 1320d et seq. https://www.law.cornell.edu/uscode/text/42/1320d
See also, 45 C.F.R. pts. 160, 164 (HIPAA privacy and security rules; breach notification provisions). https://www.law.cornell.edu/cfr/text/45/part-160

[12] 15 U.S.C. § 1681 et seq. (Fair Credit Reporting Act). https://www.law.cornell.edu/uscode/text/15/1681

[13] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 5 - 6 (core processing principles and lawful bases). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

diligence without a clear necessity, without defined retention windows, or without adequate transparency and lawful basis analysis. When that happens, an effort to reduce fraud risk can create privacy exposure, including enforcement risk and cross-border transfer problems.

A practical example is when a firm adopts enhanced biometric or device-based identity verification for remote signing: it may improve fraud detection but also expand the firm's personal data footprint, vendor dependencies, and cross-border transfer obligations.

Professional conduct rules then overlay all of these regulatory demands and introduce a unique risk for legal professionals: attorneys must reconcile duties of confidentiality, loyalty, and competence with the practical need to detect fraud, prevent misuse of client funds, and avoid assisting unlawful conduct. The duty of competence, expressly stated in the ABA Model Rules, has increasingly been interpreted to include technology literacy and an understanding of modern risks that materially affect representation.[14] In the synthetic identity context, this means lawyers may be criticized not just for failing to catch a sophisticated fraud, but also for failing to implement reasonable safeguards, failing to train staff, failing to supervise vendors, or failing to respond appropriately once red flags appear.

[14] American Bar Association (ABA) 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; see also Comment 8 (maintaining competence includes keeping abreast of relevant technology). https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/

Confidentiality adds another dimension because any internal escalation or investigation must be handled in a way that limits dissemination of client information while still enabling effective risk management.[15]

Trust account and property protection obligations further elevate the stakes in funds-handling matters, because misdirected client funds- whether caused by wire fraud, synthetic identities, or vendor compromise, can trigger severe disciplinary consequences even when the lawyer did not intend harm.[16]

The overall compliance reality is that synthetic identity fraud cannot be addressed through a single "fraud policy" document. Effective compliance requires an integrated framework: onboarding and beneficial ownership diligence, data governance and security controls, vendor oversight, escalation procedures, incident response readiness, and professional responsibility alignment. For legal professionals, the "best" compliance posture is one that can be defended after the fact. Regulators and courts do not require perfection, but they do scrutinize whether policies existed, were enforced and were documented. A firm that can demonstrate reasonable and applied controls- especially around identity verification and funds transfers, will

---

[15] ABA 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/

[16] ABA 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/
ABA 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/

be better positioned to reduce losses and to defend itself when synthetic identity fraud tests the balance between efficient legal practice and thorough identity verification.

V. Key Legal Cases and Enforcement Actions

Although synthetic identity fraud is a comparatively recent and fast-evolving risk, U.S. courts and regulators are increasingly addressing the legal failures that allow it to succeed: inadequate identity verification, weak controls over high-value disbursements, insufficient supervision of staff and vendors, and poor incident response. For legal professionals, the most important "case law" is often not a headline-grabbing decision labeled "synthetic identity fraud," but rather a body of opinions and enforcement actions that allocate loss, impose duties of care, and measure firms' reasonableness when an imposter or fabricated identity causes financial harm. The clear trend is that courts and regulators are less sympathetic to the argument that "a criminal did this to us," and more focused on whether the legal professionals involved were in the best position to prevent the loss, whether they ignored red flags, and whether they employed verifiable firm-wide controls consistent with modern risk realities.

One of the notable decisions for lawyers handling settlements and disbursements is the recent, *Thomas v. Corbyn Restaurant Development Corp.* (2025), a California Court of Appeal case arising from a spoofing scheme that diverted settlement funds. The parties resolved a personal injury matter for $475,000, with payment specified to be made to plaintiff's counsel's client trust account by check. After the settlement, an unknown third party impersonated plaintiff's counsel and transmitted fraudulent wire instructions to defense counsel, which defense counsel ultimately followed, resulting in the loss of the funds. The Court of Appeal affirmed an

order requiring the defendants to pay the settlement amount again, emphasizing that red flags existed and that the paying side's failure to exercise ordinary care contributed to the loss.[17] The opinion has become a notable reference point precisely because it treats the imposter event as a foreseeable risk of modern practice rather than an unforeseeable anomaly. In practical terms, it signals that parties who deviate from agreed payment methods or fail to confirm changed instructions may be treated as the loss-bearing party.

A related and widely cited decision in the escrow account handling is *Mago v. Arizona Escrow & Financial Corp.*, where funds were diverted through an email-based imposter scheme and a jury allocated 100% fault to the escrow agent. The Arizona Court of Appeals upheld the jury's ability to allocate full fault to the professional intermediary even though the underlying fraudster was the primary wrongdoer. The underscoring practical reality for attorneys and other gatekeepers is that fraudsters are frequently uncollectible, their location is unknown, and courts may look to the intermediary as the party for loss allocation and deterrence.[18]

For lawyers, the lesson is not limited to escrow companies. It has direct implications for law firms that function as settlement payees, escrow holders, or fiduciaries over client funds. If a firm's internal controls permit last-minute changes to wiring instructions based on email-only communications or unverified "authority" claims, the firm's exposure can shift from "victim of a

---

[17] *Thomas v. Corbyn Restaurant Dev. Corp.,* 111 Cal. App. 5th 439 (Cal. Ct. App. May 27, 2025). https://cases.justia.com/california/court-of-appeal/2025-d083655.pdf?ts=1748363463

[18] *Mago v. Arizona Escrow & Fin. Corp.,* No. 1 CA-CV 22-0270 (Ariz. Ct. App. Mar. 30, 2023). https://cases.justia.com/arizona/court-of-appeals-division-one-unpublished/2021-1-ca-cv-19-0753.pdf?ts=1614882659

scam" to "entity that failed to exercise ordinary care." Those conclusions can then escalate into malpractice claims, breach of fiduciary duty allegations, and trust-account disciplinary inquiries, particularly where clients argue that a lawyer's role as fiduciary imposes heightened diligence obligations.

While the most visible litigation involving imposters often appears in wire diversion cases, synthetic identity fraud has also driven broader regulatory scrutiny of identity verification systems within the consumer finance ecosystem, with consequences that affect legal professionals. Although these actions may not always use the phrase "synthetic identity fraud," they reflect the same regulatory posture: firms must build processes capable of detecting identity manipulation, responding to disputes, and correcting errors, especially where identity fraud leads to wrongful collection, inaccurate reporting, or consumer harm. This posture matters for lawyers in at least three ways. First, law firms advising regulated clients must anticipate that identity verification is not merely an operational issue, but a legal compliance issue under statutes such as the Fair Credit Reporting Act[19] and the Consumer Financial Protection Act.[20] Second, when legal departments oversee vendor relationships- identity verification vendors, consumer reporting services, onboarding vendors, regulators may evaluate whether the organization's legal function ensured adequate governance, escalation paths, and documentation. Third, when identity failures result in consumer injury, counsel may face discovery and reputational risk if internal

[19] 15 U.S.C. § 1681 et seq. (Fair Credit Reporting Act).

[20] 12 U.S.C. § 5531 (Consumer Financial Protection Act), Unfair, Deceptive, or Abusive Acts or Practices (UDAAP authority); and related provisions. Statutory references provided for compliance anchoring. https://uscode.house.gov/view.xhtml?req=(title:12%20section:5531%20edition:prelim)

communications suggest the legal team treated identity anomalies as a cost of doing business rather than a compliance priority.

Federal guidance and typology publications also signal increasing governmental attention to synthetic identity patterns. FinCEN has publicly highlighted identity manipulation techniques-particularly those involving altered or fabricated identity documents and advanced deception methods, as part of its broader anti-money laundering and suspicious activity reporting domains. In a 2024 alert addressing deepfake-enabled fraud, FinCEN explicitly referenced "synthetic identity" concepts and described how criminals use falsified media and documents to circumvent identity verification and authentication controls.[21] Even though these alerts are directed primarily to financial institutions, they shape expectations for gatekeepers and intermediaries, including attorneys working in high-risk transactional spaces. Practically, such guidance increases the likelihood that banks will demand more robust identity verification and beneficial ownership clarity as a condition of closing or funding transactions, and it increases the risk that a law firm will be scrutinized when a transaction it facilitated later appears in suspicious activity reporting or enforcement investigations.

At the consumer protection and data security level, the Federal Trade Commission continues to be a core national actor. The FTC's enforcement authority against unfair or deceptive acts or practices under Section 5 of the FTC Act is routinely invoked in privacy and security enforcement matters.[22] This matters because synthetic identity fraud is often enabled by

---

[21] *FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions*, FIN-2024-Alert004, (November 13, 2024). https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

[22] 15 U.S.C. § 45(a) Federal Trade Commission Act (prohibiting unfair or deceptive acts or practices). FTC privacy and security enforcement posture.

weak data security, poor access controls, or insufficient vendor oversight: when sensitive intake data is compromised or manipulated, the same incident can become both an identity fraud event and a data security event.

For law firms, this creates an enforcement risk. A single synthetic identity incident can trigger questions not only about verification adequacy and funds transfer procedures, but also about whether the firm maintained reasonable safeguards for nonpublic personal information, whether it overshared data with vendors, and whether it implemented basic security governance consistent with national expectations reflected in FTC standards and state laws.

The practical takeaway across these cases and enforcement trends is that synthetic identity fraud is being absorbed into a broader "reasonableness" framework. Courts increasingly look for ordinary-care measures such as confirming changed payment instructions through reliable channels and reacting appropriately to red flags. Regulators increasingly expect documented programs that prevent, detect, and respond to identity anomalies, supported by training, vendor oversight, and audit trails. For legal professionals, the consequence is that synthetic identity fraud is not treated as a purely criminal external risk; it is treated as an operational and compliance risk that must be governed like other foreseeable risks in modern legal practice.

VI. Ethical and Professional Responsibility Implications

Synthetic identity fraud presents a direct challenge to several ethical principles of the legal profession, particularly competence, confidentiality, loyalty, and independent professional judgment. As legal practice becomes increasingly digital and relies more heavily on electronic

verification and remote interaction, ethical compliance can no longer be separated from a lawyer's understanding of how modern fraud schemes operate. Courts, regulators, and disciplinary authorities have begun to treat synthetic identity fraud as a foreseeable hazard of contemporary legal practice- one that lawyers are expected to understand and manage within the bounds of professional responsibility.

The duty of competence is the ethical obligation most directly implicated. Under the ABA Model Rules of Professional Conduct, competent representation requires not only substantive legal knowledge, but also the "thoroughness and preparation reasonably necessary for the representation."[23] This duty has been interpreted to include technological literacy and an understanding of risks associated with the use of technology in legal practice.[24] In the context of synthetic identity fraud, competence requires that lawyers understand, at a functional level, how synthetic identities are created, how they can pass document-based verification, and how they are commonly used to exploit legal and financial systems. A lawyer who relies only on facially valid identification documents, automated verification results, or third-party assurances may be criticized for failing to exercise reasonable professional judgment if those tools are known to be vulnerable to manipulation.

For example, in a real estate closing or corporate formation matter, a lawyer who assists in structuring a transaction without understanding how synthetic identities are used to mask beneficial ownership may inadvertently facilitate fraud or money laundering. Similarly, a litigation attorney who accepts a client's asserted identity and authority without reasonable

---

[23] American Bar Association (ABA) Model Rule 1.1: *Competence, Client-Lawyer Relationship.*

[24] *Ibid*.

inquiry- particularly where inconsistencies exist, may later face questions about whether the Federal Rules of Civil Procedure, Rule 11 obligations or analogous state rules were satisfied.[25] In these scenarios, the ethical inquiry does not turn on whether the lawyer could have perfectly detected the fraud, but whether the lawyer took reasonable steps, consistent with modern practice standards, to understand and mitigate known risks.

Confidentiality obligations further complicate a lawyer's response to suspected synthetic identity fraud. ABA Module Rule 1.6 broadly prohibits disclosure of information relating to the representation of a client, subject to limited exceptions. When a lawyer begins to suspect that a client may be a synthetic identity or that the representation is being used to facilitate fraud, the lawyer must carefully maintain the balance between protecting client confidentiality and preventing harm. Enhanced verification measures- such as requesting additional documentation, confirming authority through independent channels, or involving internal compliance personnel, may be ethically permissible and even required. In addition, they must be undertaken in a manner that respects confidentiality and avoids unnecessary disclosure.

Moreover, reporting obligations often intersect with professional secrecy. While U.S. lawyers are generally not subject to the same mandatory suspicious activity reporting (SARs) requirements imposed on banks under the Bank Secrecy Act, certain practice contexts and jurisdictions impose obligations that can override or affect confidentiality. For example, some rules and ethics opinions permit or require disclosure to prevent a client from committing a crime

[25] Federal Rules of Civil Procedure 11(b).

or fraud that is reasonably certain to result in substantial financial injury, particularly where the lawyer's services are being used to further that conduct.[26]

Synthetic identity schemes can obscure conflicts of interest by presenting multiple fabricated entities or individuals as unrelated clients or counterparties, when in fact they are controlled by the same fraudster behind them. A lawyer who fails to identify these artificial relationships may unknowingly represent adverse interests, facilitate self-dealing transactions, or compromise the integrity of the representation.

For example, a synthetic identity may be used to create multiple shell entities that appear as independent buyers and sellers in a transaction, or as separate plaintiffs in coordinated litigation. Without due diligence, a lawyer may accept representations that mask common control or fabricated distinctions, thereby undermining conflict checks and exposing the firm to disqualification motions, penalties, or disciplinary scrutiny.

Ultimately, the ethical implications of synthetic identity fraud reinforce a broader trend in professional responsibility: lawyers are expected to anticipate and manage foreseeable risks created by the tools and systems they choose to use. Efficiency, client convenience, and technological adoption do not excuse ethical blind spots. Instead, ethical compliance increasingly requires an integrated approach that combines legal judgment, technological awareness, and institutional safeguards. Lawyers who understand this shift and implement reasonable, documented controls are far better positioned to protect their clients, their firms, and their professional standing in an environment where identity itself is manipulated.

---

[26] ABA Model Rule 1.6(b)(2)–(3) (permitting disclosure to prevent or mitigate client crime or fraud causing substantial financial injury when the lawyer's services have been used).

VII. Operational Challenges for Law Firms and Legal Departments

From an operational standpoint, synthetic identity fraud compels law firms and legal departments to examine workflows that were designed for efficiency rather than risk resilience. Over the past decade, the legal industry has rapidly adopted remote work arrangements, virtual notarization, electronic signatures, cloud-based document management, and digital client portals. These tools have delivered undeniable benefits in speed, accessibility, and cost reduction, but they have also expanded the attack areas available to fraudsters. Synthetic identity schemes thrive in environments where identity reviews are accepted through digital channels without corroboration through independent or contextual verification. A fraudster who successfully presents a synthetic identity through remote onboarding can interact with the firm for months without ever appearing in person, gradually building credibility and trust before exploiting that access to divert funds, extract confidential information, or manipulate legal processes.

Remote work and virtual client engagement may illustrate this challenge. When attorneys and staff communicate primarily through email, messaging platforms, and videoconferencing, traditional informal safeguards- such as in-person recognition, physical documents, or office-based verification, are diminished. Fraudsters using synthetic identities can exploit these gaps by impersonating clients or authorized representatives, particularly when staff are under time pressure or managing high volumes of digital communications. For example, a synthetic identity posing as a corporate officer may request urgent changes to transaction documents or payment instructions, relying on the absence of face-to-face interaction to avoid scrutiny. If the firm's operational procedures permit reliance primarily on email confirmations or scanned documents alone, the fraudster's fabricated identity may go unchallenged until after losses occur.

Virtual notarization and electronic signature platforms present similar operational risks. While these tools are legally recognized under federal and state law frameworks such as the Electronic Signatures in Global and National Commerce Act and the Uniform Electronic Transactions Act, their effectiveness depends heavily on identity verification processes.[27] When those processes rely on knowledge-based authentication or document uploads that can be manipulated using synthetic identities, the legal validity of the signature does not necessarily include the authenticity of the signer. Law firms that treat e-signature completion as conclusive proof of identity may inadvertently facilitate fraudulent transactions, estate planning documents, or settlement agreements, later facing disputes over enforceability and allegations that firms failed to exercise reasonable care in verifying the signer's identity.

Digital client portals and cloud-based systems introduce additional operational risk. These platforms centralize large volumes of sensitive personal and financial information, making them attractive targets for fraudsters seeking to leverage synthetic identities to gain unauthorized access. A synthetic identity that passes online verification may be granted credentials to a client portal, from which the fraudster can monitor communications, download documents, or initiate instructions that appear legitimate. If access controls are weak or monitoring is insufficient, such activity may go unnoticed. When a breach or misuse is discovered, the law firm may face not

---

[27] 15 U.S.C. §§ 7001–7031. https://www.law.cornell.edu/uscode/text/15/7001
See also, Electronic Signatures in Global and National Commerce Act (2000). https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf
Also, Uniform Electronic Transactions Act (1999), adopted in various forms by most U.S. states. https://content.next.westlaw.com/Glossary/PracticalLaw/I66e3df587a6611e498db8b09b4f043e0?transitionType=Default&contextData=(sc.Default)

only fraud-related losses but also data security and breach notification obligations under privacy statutes and contractual commitments to clients.

The operational risks are compounded by the widespread use of third-party vendors. Identity verification services, document management platforms, e-discovery providers, payment processors, and cloud hosting services are now integral to legal practice. While outsourcing can enhance capabilities, it does not transfer responsibility. Law firms remain accountable for the consequences of vendor failures, particularly when those failures involve identity verification or the safeguarding of client funds and data. Regulatory frameworks and professional standards consistently emphasize that delegation does not eliminate responsibility. For example, under federal information security expectations reflected in statutes such as the Gramm-Leach-Bliley Act and its implementing Safeguards Rule, covered entities must oversee service providers and ensure they maintain appropriate protections.[28] Even where a law firm is not directly subject to GLBA, courts and regulators increasingly use similar standards to assess whether the firm exercised reasonable care in vendor selection and oversight.

A common operational failure arises when firms adopt identity verification tools without fully understanding their limitations. Many services are designed to reduce friction by approving identities that meet minimum thresholds, but synthetic identities are often engineered precisely to meet those thresholds. If a firm treats vendor approval as a substitute for internal judgment, rather than as one step into a broader verification process, it risks running into compliance failures. For example, a vendor may verify an identity for onboarding, another vendor may

---

[28] 15 U.S.C. §§6801-6809, Gramm-Leach-Bliley Act (privacy and safeguards provisions). See also 16 C.F.R. pt. 314 (FTC Safeguards Rule under GLBA authority).

process payments based on that onboarding, and a document management system may grant access based on the same credentials. When the identity later proves to be synthetic, each process becomes a point of exposure, and the firm may be criticized for failing to implement layered controls or to reassess risk as the relationship evolved.

Training and awareness represent perhaps the most persistent operational challenge. Synthetic identity fraud is hard to detect. Fraudsters often avoid obvious red flags such as inconsistent names or clearly falsified documents, instead presenting internally consistent but fabricated profiles that withstand a quick review. Attorneys and staff who are not trained to recognize behavioral indicators- such as unusual urgency, reluctance to engage in live verification, or transaction patterns that do not align with the stated legal objective, may miss warning signs. Moreover, legal professionals are often conditioned to trust client representations and to prioritize responsiveness, a legal practice dynamic that fraudsters actively exploit. Continuous education and training are therefore essential. Moreover, one-time training sessions or static policy documents are insufficient to maintain awareness in a rapidly evolving threat environment. Scenario-based training that reflects real-world workflows- client intake, settlement disbursement, entity formation, and remote execution of documents, helps personnel internalize how synthetic identity fraud actually affects legal practice. From a compliance perspective, documented training programs also serve as evidence of fraud risk management. When disputes or investigations arise, the firm's ability to demonstrate that it trained its personnel, updated procedures, and reinforced escalation expectations can significantly influence assessments of reasonableness and liability.

As discussed, operational challenges associated with synthetic identity fraud cut across technology, vendors, personnel, and culture. Legal organizations must balance efficiency with verification, convenience with control, and delegation with oversight. Federal statutes governing electronic transactions, data security, and consumer protection provide the legal backdrop against which these operational choices are evaluated, but the decisive factor in many cases is whether the law firm implemented consistently enforced processes that reflect an understanding of modern fraud risks. As synthetic identity schemes become more sophisticated, operational resilience- supported by training, oversight, and adaptive workflows, becomes a core component of professional responsibility and risk management.

VIII. Risk Mitigation and Strategic Responses

Effectively addressing synthetic identity fraud requires a layered, risk-based approach that integrates legal judgment, technological safeguards, and organizational governance. No single control is sufficient to prevent or detect synthetic identities, particularly because these schemes are intentionally designed to evade point-in-time verification. Instead, resilience depends on combining multiple controls that operate at different stages of the client relationship and transaction lifecycle. For legal professionals, this means moving beyond isolated compliance measures and adopting an integrated framework in which attorneys, compliance officers, information technology teams, finance personnel, and external experts collaborate to identify risk, implement controls, and respond decisively when anomalies arise.

At the front end of the relationship, enhanced client onboarding procedures are critical. Traditional onboarding often focuses on documentary verification, such as reviewing

government-issued identification or formation documents. While necessary, these measures are increasingly insufficient on their own. Synthetic identities are frequently engineered to pass document-based checks, especially when verification relies on static identifiers that can be obtained, fabricated, or reused. A risk-based onboarding framework therefore supplements document review with behavioral analysis and contextual assessment. For example, legal teams should evaluate whether the proposed transaction aligns with the client's stated background, business purpose, and financial profile. A newly formed entity seeking to engage in a complex, high-value transaction with compressed timelines may warrant additional scrutiny, even if formation documents appear valid. Similarly, inconsistencies in communication patterns, reluctance to participate in live verification, or repeated reliance on intermediaries may signal elevated risk. This type of contextual review aligns with broader federal expectations that customer due diligence should be proportionate to risk, an approach reflected in anti-money laundering principles under the Bank Secrecy Act.[29]

Effective onboarding also requires continuity rather than a one-time check. Synthetic identity fraud often unfolds over time, with fraudsters cultivating legitimacy through repeated interactions. Legal teams should therefore reassess identity and authority at key milestones, such as before significant fund transfers, execution of critical documents, or material changes in transaction scope. This approach mirrors national compliance expectations in other regulated sectors, where ongoing monitoring is treated as an essential complement to initial verification.

---

[29] 31 U.S.C. §§ 5311–5336; 31 C.F.R. Chapter X (Bank Secrecy Act framework emphasizing risk-based customer due diligence and monitoring).

From a strategic perspective, periodic reassessment reduces the likelihood that early-stage verification errors will compound into large losses later in the relationship with clients.

Controls governing trust accounts and fund transfers are another central pillar of risk mitigation. Because client funds are particularly attractive targets for synthetic identity schemes, policies in this area should be intentionally conservative. Segregation of duties is one of the most effective safeguards: no single individual should be able to initiate, approve, and execute a funds transfer without independent review. Multi-factor authentication (MFA) for access to banking platforms and payment systems further reduces the risk that compromised credentials tied to a synthetic identity can be used to move funds. Perhaps most critically, law firms should require mandatory verification of any change to payment instructions through an independent and reliable channel, such as a verified telephone call using contact information already on file rather than information provided in the change request. These measures are consistent with the fiduciary principles underlying client trust account obligations and with the heightened care expected when handling client property under professional conduct rules.[30] They also align with regulatory expectations reflected in consumer protection and financial security frameworks, which emphasize internal controls designed to prevent unauthorized transfers and mitigate foreseeable fraud risks.[31]

Strategic risk mitigation extends beyond individual transactions to firm-wide governance. Law firms and legal departments should document their approach to fraud risk through formal risk assessments, written policies, and incident response plans. A documented fraud risk

---

[30] ABA Model Rule 1.15: *Safekeeping Property, Client-Lawyer Relationship.*

[31] See, e.g., consumer protection and financial security expectations enforced under 15 U.S.C. § 45(a) (FTC Act) and related guidance addressing unfair practices and inadequate controls.

assessment identifies practice areas, transaction types, and workflows that present elevated exposure, such as real estate closings, settlement disbursements, entity formation, or cross-border matters. Incident response plans establish clear escalation paths, decision-making authority, and communication protocols so that personnel do not have to improvise under pressure. Compliance protocols translate these assessments into operational expectations, training requirements, and monitoring mechanisms. From a regulatory and litigation standpoint, documentation serves a dual purpose: it improves operational readiness and provides evidence that the firm took reasonable steps to identify and mitigate known risks.

In disputes arising from fraud losses, courts and regulators routinely examine whether policies existed, whether they were communicated, whether personnel were trained, and whether the policies were followed in practice. The absence of documentation can be interpreted as the absence of controls, even if informal practices existed. By contrast, a firm that can demonstrate a structured, risk-based program- supported by training records, escalation logs, and periodic review, will be better positioned to defend against allegations of negligence, breach of fiduciary duty, or failure to supervise. This concept of documented reasonableness is embedded throughout U.S. compliance regimes, including information security standards under the Gramm-Leach-Bliley Act's Safeguards Rule, which emphasizes written programs, risk assessment, and ongoing evaluation as hallmarks of reasonable protection for sensitive information.[32]

[32] 15 U.S.C. §§6801-6809, Gramm-Leach-Bliley Act (privacy and safeguards provisions).

Ultimately, risk mitigation and strategic response to synthetic identity fraud require a firm's cultural shift as much as a technical one. Collaboration across disciplines, layered controls tailored to risk, and robust documentation together form a defensible posture that acknowledges the realities of modern fraud without sacrificing the efficiency and trust essential to legal practice. As synthetic identity schemes continue to evolve, firms that embed these principles into their operational and governance structures will be best positioned to reduce losses and withstand regulatory, legal, and reputational scrutiny.

IX. Conclusion

Synthetic identity fraud represents a significant challenge for the legal profession, one that reflects broader changes in how identity and trust function in an increasingly digital economy. Unlike traditional forms of fraud that rely primarily on deception or the misuse of a single individual's credentials, synthetic identity fraud is deliberately engineered to appear legitimate. It exploits the systems that legal professionals rely on for efficiency and access, including remote onboarding, electronic signatures, digital payment platforms, and automated verification tools. As a result, it undermines long-standing assumptions about how identity is established and verified within legal practice, forcing lawyers to confront risks that are persistent and often invisible until significant harm has already occurred.

The deceptive nature and technological sophistication of synthetic identity fraud mean that reactive responses are no longer sufficient. Legal professionals can no longer treat identity verification as a peripheral administrative function delegated to intake staff, vendors, or automated systems. Instead, identity verification has become a core component of professional

responsibility, risk management, and client protection. It implicates duties of competence, confidentiality, supervision, and fiduciary care, and it intersects with regulatory regimes governing financial crime prevention, data security, consumer protection, and corporate transparency. When identity fails, the consequences can escalate across these domains, resulting in financial loss, regulatory scrutiny, malpractice exposure, and reputational damage that far exceeds the cost of preventative measures.

A meaningful response to synthetic identity fraud requires both knowledge and firm-wide commitment. Legal professionals must understand how synthetic identities are created and cultivated, how they evade traditional verification, and how they are deployed across legal and financial systems. They must stay informed about evolving regulatory expectations, including developments in beneficial ownership reporting, data protection, and enforcement priorities that increasingly emphasize preventative controls and governance. Emerging case law and enforcement actions demonstrate that courts and regulators are less willing to treat fraud as an uncontrolled external risk and more inclined to scrutinize whether lawyers and firms implemented reasonable, risk-based safeguards consistent with modern practice realities.

Equally important is the strengthening of internal controls and organizational culture. Policies governing client intake, trust accounts, vendor oversight, staff training and incident response must be documented, communicated, and enforced in practice, not merely adopted in theory. Training must be continuous and practical, equipping attorneys and staff to recognize the red flags and to escalate concerns without fear of reprisal. Senior partners and firms' governance structures must ensure accountability at the leadership level, reinforcing the principle that fraud prevention is a shared responsibility rather than an isolated compliance function.

Ultimately, how legal professionals respond to synthetic identity fraud will shape the outcomes. Lawyers serve as essential intermediaries in dispute resolution, real estate and M&A transactions, financial markets, corporate governance, and the administration of justice. If synthetic identities can reliably pass through legal systems unchecked, public confidence in those systems erodes. Conversely, when legal professionals embrace their evolving role as informed gatekeepers- integrating legal judgment with technological awareness and robust risk management, they help preserve the integrity of legal institutions and the trust upon which they depend. In modern times, when identity itself can be manufactured, the profession's commitment to diligence, reasonableness, and ethical responsibility becomes a defining measure of its continued credibility.

X. References

Statutes

12 U.S.C. § 5531 (Consumer Financial Protection Act), Unfair, Deceptive, or Abusive Acts or Practices (UDAAP authority); and related provisions. Statutory references provided for compliance anchoring. https://uscode.house.gov/view.xhtml?req=(title:12%20section:5531%20edition:prelim)

15 U.S.C. § 45(a) Federal Trade Commission Act (prohibiting unfair or deceptive acts or practices). https://www.law.cornell.edu/uscode/text/15/45

15 U.S.C. Chapter 96 Electronic Signatures in Global and National Commerce Act (2000). https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf

15 U.S. Code § 1681m - Requirements on users of consumer reports (e) Red flag guidelines and regulations required https://www.law.cornell.edu/uscode/text/15/1681m

15 U.S.C. § 1681 et seq. (Fair Credit Reporting Act). https://www.law.cornell.edu/uscode/text/15/1681

15 U.S.C. §§6801-6809, Gramm-Leach-Bliley Act (privacy and safeguards provisions). https://www.notarylearningcenter.com/pdf/GrammLeachBliley.pdf

15 U.S.C. §§ 7001–7031. https://www.law.cornell.edu/uscode/text/15/7001

31 U.S.C. §§ 5311–5336; 31 C.F.R. Chapter X (Bank Secrecy Act and FinCEN regulations). https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X

31 U.S.C. § 5336 Corporate Transparency Act; beneficial ownership information reporting requirements. https://www.law.cornell.edu/uscode/text/31/5336

42 U.S.C. § 1320d et seq. https://www.law.cornell.edu/uscode/text/42/1320d

Uniform Electronic Transactions Act (1999), adopted in various forms by most U.S. states. https://content.next.westlaw.com/Glossary/PracticalLaw/I66e3df587a6611e498db8b09b4f043e0?transitionType=Default&contextData=(sc.Default)

Rules and Regulations

16 C.F.R. pt. 314 (FTC Safeguards Rule under GLBA authority). https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf

16 C.F.R. § 681.1 (identity theft prevention programs—"Red Flags Rule"). https://www.law.cornell.edu/cfr/text/16/681.1

45 C.F.R. pts. 160, 164 (HIPAA privacy and security rules; breach notification provisions). https://www.law.cornell.edu/cfr/text/45/part-160

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/*

Federal Rules of Civil Procedure 11(b) (requiring reasonable inquiry and factual support for pleadings and representations to the court). https://www.law.cornell.edu/rules/frcp/rule_11

Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 5–6 (core processing principles and lawful bases). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Cases

Mago v. Arizona Escrow & Fin. Corp., No. 1 CA-CV 22-0270 (Ariz. Ct. App. Mar. 30, 2023). https://cases.justia.com/arizona/court-of-appeals-division-one-unpublished/2021-1-ca-cv-19-0753.pdf?ts=1614882659

Thomas v. Corbyn Restaurant Dev. Corp., 111 Cal. App. 5th 439 (Cal. Ct. App. May 27, 2025). https://cases.justia.com/california/court-of-appeal/2025-d083655.pdf?ts=1748363463

Reports

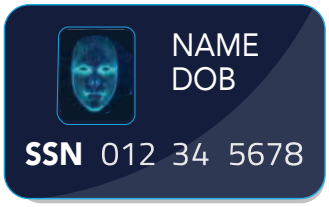
FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004, (November 13, 2024). https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

While the execution of synthetic identity fraud can be quite complex, certain factors aid in the creation of synthetic identities, often making it more attractive to fraudsters than many other types of fraudulent activity. From the foundational way the United States approaches identities to the processes in place to build and foster credit, fraudsters zero in on opportunities to not only create, but quickly establish a synthetic identity in the payment system.

USE OF SOCIAL SECURITY NUMBERS AS A PRIMARY IDENTIFIER

Synthetic identities tend to be more prevalent in the United States than in other countries due in part to a strong reliance on Social Security numbers (SSNs) as identifiers.



SSNs were initially created by the Social Security Administration (SSA) for a very specific purpose: tracking earnings histories of individuals for use in determining Social Security benefits. Over time, the use of SSNs has expanded substantially to become an almost de facto universal identifier in the United States.

The problem with reliance on a static national identifier, such as the SSN, is that a compromised SSN can be used by fraudsters to take over an identity, or in the case of synthetic identity fraud, create a new identity under the guise of an existing SSN. SSNs also are hard to validate, as there is not currently a real-time mechanism for institutions to confirm the provided SSN matches other customer information on an application.

Then, beginning in 2011, the randomization of SSN assignment affected SSN validation processes. ***According to the SSA***, randomization was implemented to protect the integrity of SSNs and to extend the pool of nine-digit SSNs available nationwide. Randomization eliminated the geographical significance of the first three digits of the SSN (also called the area number), which financial institutions previously used when attempting to determine the SSN's state of origin.

ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

IMPROVED SSN VERIFICATION ON THE HORIZON

To help control fraud related to SSNs, the SSA introduced a written ***Consent Based Social Security Number Verification (CBSV)*** service in 2008. This service enables paid subscribers to verify a name, date of birth and SSN match the SSA's records with written consent from the SSN holder. A challenge of this paper-based process was the requirement of a physical, or "wet," signature from the SSN holder. This often took time to obtain and submit for verification processing. An ***electronic version of this verification process*** was introduced as part of a pilot program by the SSA in 2020, allowing the use of electronic signatures for consent and therefore, quicker submission and processing times for verification. The pilot program initially launched with a limited number of permitted entities (10) but expanded rollout in 2021. The ability for institutions to validate key identity elements of a customer when processing an application will enable them to better identify potential synthetic identities up front, preventing them from entering the institution's portfolio.

SOME SSNS ARE MORE ATTRACTIVE TO FRAUDSTERS

In the creation of synthetic identities, fraudsters often will leverage an SSN that is not tied to an active credit profile. This includes SSNs issued to children, the incarcerated and the elderly, as fraudsters rely on the fact that these populations do not regularly use or monitor their credit.

FREQUENT DATA BREACHES / INCREASED AVAILABILITY OF PERSONAL INFORMATION TO FRAUDSTERS

A record number of data breaches over the past few years have placed valuable personally identifiable information (PII) at fraudsters' fingertips. According to ***the Identity Theft Resource Center***, records of more than 300 million individuals were exposed in 2020 alone as a result of data breaches. The information obtained from these data breaches is often shared among criminals on the "dark web" – a subset of the internet inaccessible by traditional browsers and search engines, and where content and activities are anonymous. Information readily available for purchase includes bank login credentials, account information, driver's license numbers, credit card numbers and SSNs. Other popular means for obtaining PII include social engineering or simply collecting information shared on social media. There is no shortage of data available to fraudsters wishing to create a synthetic identity using real or modified information.

ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

CREDIT APPLICATION PROCESSES WORK TO THE FRAUDSTER'S ADVANTAGE

- **Credit file creation:** After the initial creation of a synthetic identity, certain required credit processes can help facilitate the introduction of the synthetic identity into the payment system. Upon initial creation, the synthetic identity has no purchasing power, so the fraudster often initiates a credit application. Even if a credit application is rejected, the credit reporting agencies (CRAs) automatically create a new credit profile, since the applicant is considered to be both new and a real person. (This is a requirement of the ***Fair Credit Reporting Act***, which mandates that CRAs create a profile for an individual if none exists.) The new credit profile creates an identity marker which becomes the synthetic identity's so-called "proof" of existence. The fraudster then continues to apply for credit until eventually approved. The credit bureau assumes the first applicant using a given SSN is legitimate. Any other individual who applies for credit using the same SSN then must prove his or her identity – including the actual person whose SSN was stolen.

- **Credit scoring and authorized users:** Several considerations factor into a credit score, including payment history, credit utilization and length of credit history. While fraudsters may choose to build up a synthetic's creditworthiness over time, they also may act on more immediate ways to boost the identity's credit score. "Piggybacking" involves becoming an authorized user to another individual's account with good credit. In many cases, the authorized user then acquires the established credit history of the primary user, rapidly building a positive credit score. Fraudsters will go as far as to pay to be added as an authorized user to unsuspecting consumers with good credit, which expedites the credit boosting process. For the less patient fraudsters, this approach provides a more profitable synthetic in a shorter amount of time.

LIMITED VERIFICATION OF IDENTITIES

Synthetic identities typically will exhibit payment behavior mimicking an upstanding customer. As such, the key to detection is looking at the identity itself. However, current practices involve a limited degree of identity verification.

- **Customer onboarding:** During the onboarding process, institutions often will validate some customer information (such as name, date of birth, address and SSN), but this is not considered a thorough identity verification and often leans on a limited number of source documents that are easy to fabricate.

ALLURE OF A SYNTHETIC TO A FRAUDSTER: EASE OF CREATION

- **Ongoing authentication:** Once an account is opened, institutions tend to rely on the account opening process for identity verification and do not complete any subsequent validation or authentication of the identity. In effect, once a synthetic enters a portfolio, it can conduct activities without being identified until it's too late and a loss has been incurred.

TAKE ACTION

It is important to recognize how easy it is for fraudsters to create synthetic identities and yet, how difficult it is to detect them. If you observe fraudulent payment activity by a customer, consider the fact that your customer might not actually exist. By educating your organization about these processes, you are one step closer to helping mitigate this complex type of fraud.