Notarize, Inc. (dba Proof.com)
867 Boylston Street
Boston, MA 02116

Julie Lascar
Director, Office of Strategic Policy
Terrorist Financing and Financial Crimes
Department of the Treasury

October 17, 2025

RE: Response to Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets

Dear Director Lascar,

Proof appreciates the opportunity to respond to the Department of the Treasury's Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets.

ABOUT PROOF
Proof is the leading digital identity and transaction security platform, trusted by more than 16 Fortune 100 companies and thousands of organizations, having facilitated over $600 billion in secure digital transactions—from mortgage closings to retirement distributions.

As pioneers in digital trust infrastructure, we operate the nation's largest 24/7 online notarization network and have developed comprehensive identity verification systems that secure critical financial documents and transactions. Through partnerships across government and industry, Proof advances policies that strengthen consumer protection while enabling innovation in digital commerce.

Our response examines the identity fraud risks facing financial institutions (FIs), current innovations in digital identity verification, and the regulatory modernization needed to enable digital credentials—particularly important for detecting and mitigating illicit finance in digital assets. For more information, visit www.proof.com.

RESPONSES TO TREASURY RFC QUESTIONS

Question 1: In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem?
Identity-related fraud is the principal vulnerability enabling illicit finance across the digital asset ecosystem.

FinCEN's 2024 Financial Trend Analysis underscores this, identifying over $80 billion in suspicious activity linked to identity theft (using a customer's information without permission) and the use of false records (the altering, counterfeiting, or forging of documents).[1]

The FBI's 2024 Internet Crime Complaint Center (IC3) Report further documents billions in losses from personal data breaches and identity theft schemes, demonstrating that

[1] Financial Crimes Enforcement Network (FinCEN), Identity-Related Suspicious Activity: 2021 Threats and Trends (January 9, 2024)

compromised identification is the primary vector for illicit actors to exploit our financial system.[2]

The core of this problem is the vast amount of compromised personal data available on the dark web. This data provides the raw materials for criminals to commit sophisticated impersonation and create fraudulent documents, rendering traditional, document-centric verification increasingly ineffective. The current system perpetuates this vulnerability; every time a consumer shares identity documents with a new FI, another potential breach point is created. FinCEN itself acknowledged this risk in its June 2025 order permitting alternative TIN collection methods, noting consumer concerns over requirements to provide their complete TIN due to privacy and security risks.[3]

This foundational weakness is now being amplified by generative artificial intelligence (Gen-AI). Technologies like deepfakes exploit the very vulnerabilities of document-based systems, allowing criminals to circumvent existing checks at an unprecedented scale. Deloitte's Center for Financial Services projects that Gen-AI could enable fraud losses to reach $40 billion annually in the United States by 2027, a dramatic increase from $12.3 billion in 2023.[4] These concerns recently prompted FinCEN to issue an alert to institutions highlighting the risks from AI-generated deepfakes.[5]

Adopting persistent, verifiable digital credentials that verify attributes through privacy-protecting methods is the most effective way to address these vulnerabilities, hardening the financial system against attack and reducing massive losses from fraud.

Question 4: What innovative or novel methods, techniques, or strategies related to digital identity verification are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets?

Today, FIs deploy a multi-layered defense system of sophisticated digital identity verification and fraud monitoring methods. More recently, they have started to deploy next-generation methods that leverage digital credentials for both identity and the verification of key customer attributes. These innovations are particularly critical given the global, pseudonymous nature of blockchain transactions, which necessitate new ways to conduct verification at the points where digital assets interface with regulated financial services.

Existing Digital Identity Verification and Fraud Monitoring Methods:
FIs currently utilize several integrated technologies to establish a comprehensive and trustworthy identity profile for each customer:

> **Credential Analysis:** Automated forensic examination of government-issued IDs to detect alterations and authenticate security features against issuing authorities.

[2] Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3), 2024 Internet Crime Report (April 23, 2025)
[3] FinCEN, Exemption Order Related to TIN Collection and Customer Identification Program Requirements (OCC, FDIC, and NCUA) (June 27, 2025)
[4] Deloitte Center for Financial Services, Generative AI is expected to magnify the risk of deepfakes and other fraud in banking (May 29, 2024)
[5] FinCEN, FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions (November 13, 2024)

Biometric Comparison: Matching individuals to their government-issued IDs using live selfie capture and facial recognition, with advanced liveness detection to protect against deepfakes.

Fraud Risk Signaling: Evaluating contextual data, including device fingerprints, IP locations, and behavioral patterns, to create risk profiles that identify suspicious actors.

While these methods provide a strong baseline, the industry is evolving toward more persistent and portable solutions to address the systemic risks of redundant verification.

Emerging Digital Certificate and Credential Technologies:
The adoption of a credential-based model introduces a cascade of benefits across the entire financial ecosystem. FIs are beginning to adopt next-generation solutions to enable repeatable use of verified identities and KYC characteristics of both businesses and individuals across institutions:

For Individuals:
Digital certificates issued under the globally recognized X.509 standard provide a secure, cryptographically bound representation of a verified individual's identity. Once a consumer's identity and KYC attributes have been verified by a trusted certificate authority (CA) such as Proof, that identity is bound to a reusable digital certificate. The key to this model is its ability to cryptographically sign the transaction itself, which inseparably binds the verified identity to that specific transaction. This creates irrefutable proof of authorship and is fundamentally more secure than systems where a credential is merely presented alongside a transaction, as the cryptographic link prevents the identity from being swapped or the transaction from being repudiated. This foundational identity can then serve as a root of trust for emerging credential ecosystems, such as W3C Verifiable Credentials, ensuring they are built upon a high-assurance verification.[6]

For Entities:
The same approach applies at the organizational level. Following robust entity verification, organizations can obtain X.509 certificates to cryptographically sign a wide range of data—from static documents to dynamic transaction messages, signed attestations, or identity assertions. These signatures allow downstream recipients to verify that content originated from a verified entity. Proof, as a CA, issues entity-level certificates that can anchor various credential types, enabling institutions to leverage X.509's established trust framework as a foundation for next-generation systems that deliver the security and flexibility needed for modern financial services.

This new approach to persistent, verifiable digital credentials is particularly valuable in preventing fraud across both individual and institutional transactions. In traditional financial

[6] *See* W3C Verifiable Credentials Data Model v2.0 (2024); W3C Decentralized Identifiers (DIDs) v1.0 (2022); ISO/IEC 18013-5:2021; OpenID for Verifiable Credential Issuance (OpenID4VCI) and OpenID for Verifiable Presentations (OpenID4VP), OpenID Foundation (2023).

services, for example, when a consumer signs wire instructions with their personal digital certificate, recipients know with certainty who authorized the transfer. Similarly, when a cryptocurrency exchange provides transaction records with cryptographic signatures, recipients can instantly verify authenticity. This creates an unbreakable chain of trust that eliminates document forgery and impersonation risks that plague current systems—whether the threat comes from individuals impersonating account holders or bad actors posing as legitimate institutions. When records and data can be tied to a digital credential, it creates a verifiable record.

The evolution to persistent digital identities and cryptographically signed content represents a fundamental shift in how FIs approach identity verification, particularly crucial for digital asset transactions. Importantly, digital certificates enable trusted authorities to cryptographically sign the digital credentials they issue—providing verifiable proof that credentials originated from legitimate, verified sources. This is particularly valuable in the context of digital asset activities. For example, Proof is developing digital credentials that provide characteristic verification beyond identity – for example, the results of U.S. sanctions screening.

This approach creates an unbreakable chain of trust and provides the following potential benefits:

Enhanced Security: Digital credentials help to eliminate document forgery and create cryptographic chains of trust that dramatically reduce identity fraud in both traditional and digital asset transactions.

Reduced Costs: Eliminating redundant verification would save billions annually while reducing the operational burden on institutions and improving user experience across traditional and digital assets.

Improved Privacy: Selective disclosure and reduced document storage minimize data exposure and breach risks across the financial system.

Financial Inclusion: Streamlined verification would particularly benefit underserved populations seeking access to both traditional financial services and the digital asset economy.

Competitive Digital Asset Markets: Clear regulatory frameworks would help legitimate U.S. digital asset service providers compete with offshore platforms while maintaining strong compliance standards.

International Leadership: With the EU's eIDAS regulation, Singapore's National Digital Identity, and similar global initiatives, modernization would help the U.S. maintain leadership in both traditional financial services and the emerging digital asset economy.

Question 4(c): Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets?

Yes. Despite technological advances, FIs face challenges in adopting these innovations without clear guidance from regulators.

Systems Built for Paper in a Digital World:
Existing regulatory frameworks create unnecessary barriers to modernization:

> **Redundant Verification Requirements:** Current regulations, guidance, and, in some cases, supervisory approaches, result in each FI separately collecting and verifying the same customer information for purposes of their BSA AML and sanctions programs. When consumers interact with multiple FIs—whether traditional banks, cryptocurrency exchanges, or digital asset custodians—they must repeatedly provide documents to each institution and each of those institutions must separately verify and review the information contained in those documents. This redundancy exists because FIs do not have the guidance they need to rely on verifications performed by others for their BSA AML and sanctions programs, even when using superior digital methods and creating significant benefits in terms of accuracy and data minimization.
>
> **Digital Asset-Specific Challenges:** The real-time and pseudonymous nature of blockchain transactions makes robust identity and characteristic verification at on/off ramps particularly important for preventing illicit finance. Yet regulated cryptocurrency exchanges, wallet providers, and other digital asset service providers face the same verification requirements as traditional FIs, creating friction that may drive users to less-regulated or offshore platforms.
>
> **Consumer Burden:** Customers face repetitive, time-consuming processes that delay access to financial services and put their personal information at risk. This friction particularly impacts legitimate digital asset users who may interact with multiple platforms for trading, custody, and traditional banking services. Having to separately provide each service provider with documentation and a trove of personal information puts customers at risk for a wide variety of data breach and fraud vectors.
>
> **Institutional Costs and Risks:** FIs, whether in traditional finance or digital assets, spend billions annually on redundant verification processes while storing massive amounts of sensitive documents that create cybersecurity vulnerabilities. Every institution becomes a potential target for data breaches, with identical information stored across hundreds of organizations multiplying these risks.

Regulatory Impediments to be Addressed:
The BSA and implementing regulations were originally designed for paper-based processes. While they have evolved over time to acknowledge electronic systems that handle these same processes, existing guidance does not explicitly enable FIs to rely on digital credentials issued by third parties as part of their BSA AML or sanctions compliance programs. Current examination procedures and supervisory expectations focus on document retention rather than the effectiveness of the underlying verification. Examiners may not yet understand, or have incentive to assess, how digital credentials provide superior evidence of compliance. This creates practical impediments to the use of new innovations, including digital credentials, by FIs.

Thus, absent guidance from regulators, FIs will be slow to adopt new approaches–even where those approaches result in greater accuracy and effectiveness in their compliance programs and meaningful benefits in data minimization. Affirmative guidance from regulators is necessary to enable adoption of these modern, more effective approaches.

Question 4(d): What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets?

We encourage Treasury and FinCEN to issue regulatory guidance under the BSA permitting FIs to rely on digital credentials issued by certified credential service providers (CSPs). To be effective, this guidance should be built upon two foundational principles:

- **Support a Technology-Neutral Approach:** Rather than prescribing specific technical formats, guidance should focus on outcomes, permitting an FI to rely on any credential format that is cryptographically traceable to a certified CSP, maintains clear accountability for verification accuracy, and provides adequate audit trails.
- **Support Existing Frameworks for Certification:** Rather than creating a new governmental body, guidance should leverage existing non-governmental certification bodies like the Kantara Initiative to define requirements for CSP certification and ongoing compliance.[7]

Based on these principles, we propose the following specific language:

1. A financial institution may rely on a digital credential issued by a credential service provider (CSP) to satisfy its obligations to verify customer identity if:
    a. The CSP issues the credential pursuant to NIST Special Publication 800-63A-4 Identity Assurance Level 2 (IAL2) or a successor publication recognized by FinCEN; and
    b. The CSP maintains current certification from the Kantara Initiative under its Identity Assurance Framework for NIST 800-63A-4 or a successor assurance program recognized by FinCEN.

2. For other customer characteristics (e.g., sanctions screening results, source of funds validation, beneficial ownership verification, and other similar characteristics), a financial institution may rely on a digital credential if:
    a. The CSP employs verification processes substantially equivalent to those the financial institution would employ to perform the verification itself;
    b. The CSP maintains records of customer information and documentation it obtains and reviews in issuing the credential and makes that information available to relying financial institutions and regulators as necessary for legal, regulatory, or law enforcement purposes.

3. A financial institution may rely on a digital credential presented in any technology format, provided it is issued by a CSP that meets the requirements of this framework.

4. A CSP must:
    a. Demonstrate a cryptographically verifiable link for all verifications; and
    b. Demonstrate strong risk management and security procedures over systems and use of cryptographic keys, possess the necessary safeguards and controls to prevent misuse and exploitation, and demonstrate compliance with recognizable industry benchmarks and audits.

[7] https://kantarainitiative.org/

To advance these goals, Treasury should clarify that digital credentials can satisfy KYC elements in the Office of Foreign Assets Control's Virtual Assets Guidance, a move that would advance the dual policy goals of enforcing sanctions while protecting users from exploitative data practices. Additionally, Treasury could provide temporary safe harbors for FIs implementing these standards to accelerate adoption. A collaborative federal task force, modeled on NIST's successful NCCoE projects, could also support harmonizing regulatory approaches. By permitting the use of digital credentials for BSA compliance, Treasury would transform our financial system to enable privacy-preserving systems, instant verification without unnecessary document storage, and effective monitoring of digital asset transactions.

CONCLUSION

While FIs already deploy digital identity verification and fraud monitoring methods, regulatory clarity is essential to unlock this next chapter of innovation and unleash the full potential of digital credentials—particularly for effective use in digital asset transactions. The current system of redundant document collection burdens consumers, costs institutions billions, and creates massive security vulnerabilities that bad actors can exploit.

Treasury has the opportunity to provide guidance that would enhance security, reduce costs, protect privacy, and improve oversight of both traditional and digital asset financial services. The technology exists, the standards are mature, and the benefits are clear. What financial institutions need is regulatory clarity to confidently adopt these innovations.

We encourage Treasury to consider issuing guidance and creating frameworks that would give financial institutions the confidence to adopt digital credentials. This would be particularly valuable for improving oversight of digital asset transactions while reducing friction for legitimate users.

Proof stands ready to support Treasury in modernizing our nation's financial crime prevention infrastructure for the digital age, ensuring America leads in both traditional finance and the digital asset economy.

Should you require additional information, please contact: James Fulgenzi, Head of Public Policy at Proof: james.fulgenzi@proof.com.

Sincerely,

James Fulgenzi
Head of Public Policy
Proof