Indicio PBC
720 Queen Anne Ave. N., Unit 110
Seattle, WA 98109
www.indicio.tech

October 17, 2025

U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

Subject: Request for comment, Innovative Methods To Detect Illicit Activity Involving Digital Assets

Document Citation: 90 FR 40148
Document Number: 2025-15697

Introduction

Indicio appreciates the opportunity to comment on this regulation and is strongly interested in the advancement of digital identity frameworks that strengthen financial integrity and security. As a US-based provider of decentralized identity infrastructure and Verifiable Credential technology, Indicio develops software for financial institutions, governments, and private entities worldwide to deploy privacy-preserving digital identity verification systems that meet AML/CFT and sanctions compliance requirements. Our Indicio Proven® platform is used in production to issue and verify high-assurance digital credentials derived from trusted sources such as government eMRTDs, passport chip data, and authenticated biometrics.

These systems are already helping institutions detect and mitigate illicit finance while protecting customer privacy and ensuring regulatory auditability. Drawing on our experience implementing these solutions across financial services, system log-in authorization, and international travel programs aligned with ICAO, FATF, and NIST standards, Indicio submits this comment to share insights into how verifiable digital identity can be safely and effectively adopted to improve compliance, security, and interoperability across the financial sector.

Background

Indicio's comments address **Question 4** of the U.S. Department of the Treasury's request for information on the use of digital identity verification to detect illicit activity and mitigate illicit finance risks involving digital assets. Specifically, this section seeks input on the *innovative or novel methods, techniques, or strategies* financial institutions are using for identity verification; the *risks, benefits, challenges,* and *potential safeguards* associated with these methods; and the *portable digital identity credentialing tools* currently in use.

This topic is directly relevant to Indicio's work and expertise. Indicio develops and deploys decentralized identity infrastructure and Verifiable Credential software technology that provides high-assurance, privacy-preserving digital identity verification across borders and sectors. Our Indicio Proven® platform enables financial institutions, governments, and regulated service providers to issue, store, and verify data and identity information using tamper-proof digital credentials derived from trusted sources such as passport chips,

driver's licenses, and authenticated biometrics. These systems are in production today, supporting use cases that include anti–money laundering (AML), countering the financing of terrorism (CFT), sanctions screening, and remote onboarding.

Indicio's experience implementing interoperable, standards-based identity systems, aligned with the Financial Action Task Force (FATF) guidance for digital ID and NIST SP 800-63 digital identity assurance levels, positions us to comment on how Verifiable Credentials and portable digital identity tools can strengthen AML/CFT controls in the digital asset sector.

As digital assets move rapidly across exchanges, digital wallets, and national jurisdictions, traditional paper or database-based KYC methods leave exploitable gaps. The use of cryptographically verifiable digital credentials offers a practical and scalable path to closing those gaps while maintaining compliance, auditability, and privacy protection.

Accordingly, Indicio's comments respond to Question 4 by outlining how financial institutions can use Verifiable Credentials and other decentralized identity tools to:

- Detect and prevent illicit finance activity involving digital assets;
- Strengthen identity assurance while reducing reliance on centralized PII storage;
- Improve interoperability and auditability of AML/CFT processes; and
- Support regulatory objectives for privacy, security, and global consistency in digital identity verification.

Analysis

Use of digital assets are increasing and with that growth comes higher risk that they will be used for illicit finance. Traditional AML and KYC methods were designed for paper documents and siloed databases, which leaves gaps when digital identities can move across exchanges, wallets, and borders in seconds. That is why many leading virtual asset service providers now lean on digital identity verification that is purpose built for faster, online flows.

More large platforms, such as Indicio partner Black Mountain Investment Group, require remote KYC that includes document authentication, selfie or video checks, and sanctions screening before customers can transact. Coinbase, for example, discloses the use of third-party biometric comparison services, while Binance highlights Travel Rule obligations that require sharing sender and recipient data for certain transfers.

These are clear signs that the digital asset industry is tightening its identity controls—but also that the attack surface is expanding. Every outsourced identity verification introduces new risk: biometric data, scanned passports, and verification logs are being stored by third parties outside of the wallet provider's control. If any of those systems are compromised, hackers can weaponize that data for deepfake account takeovers, synthetic identity creation, or social engineering scams targeting investors and institutions.

Without verifiable, privacy-preserving identity credentials—where the proof of identity is cryptographically bound to the user and verified at the point of transaction—digital asset platforms are exposed to ongoing risks of impersonation, regulatory fines, and cascading trust failures. In short, centralized digital identity verification may check compliance boxes, but it also creates new honeypots for attackers and new liabilities for platforms.

Solution:

A **Verifiable Credential** is a digital, tamper-proof version of trusted information—such as a government-issued ID, passport, or license—that can be cryptographically verified to confirm authenticity. It packages identity claims in a standard format so verifiers can confirm who issued them, ensure they haven't been altered, and trust their source. By binding authoritative evidence and cryptographic checks, Verifiable Credentials make it possible to prove identity securely and reuse that proof across multiple transactions, helping prevent synthetic identities and AI-generated fraud.

Verifiable Credentials allow issuers such as banks, governments, or regulated platforms to sign attributes; holders keep those credentials in a wallet that the individual controls; verifiers check signatures and validity without relying on centralized databases for accessing source data, making them cryptographically secure and reliable while preserving the privacy of the user.

The identity data held in a Verifiable Credential can be derived from many trusted sources such as bank KYC, government ID documents, or eMRTD chip checks, then bound to authenticated biometrics and liveness receipts of an individual. Customers keep credentials in a user-controlled wallet and present only what a transaction requires, which reduces exposure of personal data and simplifies audits. Because everything is API-driven and mapped to recognized assurance frameworks, institutions can start by augmenting current AML and sanctions tools and then phase out redundant document uploads as performance is proven. This combination of portable proofs, strong assurance, and privacy by design gives the digital asset sector a practical way to close identity gaps that criminals exploit while maintaining the speed and global reach that make digital assets useful.

And because Verifiable Credentials are based on W3C standards and created from technology incubated from open source projects like Linux Foundation Decentralized Trust, they can be portable and used across institutions and jurisdictions. That portability is valuable in digital assets, where the same customer often moves between custodians, exchanges, wallets, and fiat on- and off-ramps.

Verifiable Credentials strengthen digital identity controls and align with the Financial Action Task Force's guidance for using digital ID in customer due diligence and with NIST's Digital Identity Guidelines for assurance, authentication, and federation. When institutions follow these frameworks with Verifiable Credentials, they can raise assurance while improving privacy through data minimization and clear audit trails. This technology further strengthens digital identity programs by enabling selective disclosure, a privacy-preserving method that allows an individual to share only specific, verified pieces of information from a credential such as confirming age or citizenship without revealing the entire document or other personal details.

Using Verifiable Credentials to verify identity in digital asset transactions helps to detect and mitigate illicit finance by tightening the weakest points in remote onboarding and transaction monitoring. A Verifiable Credential presentation can prove that a government document was chip-verified, that a live biometric match occurred at onboarding, and that sanctions screening was performed, all without exporting images or full PII. This reduces repeat KYC, improves sanctions hit quality, and shortens case assembly, while keeping institutions within a proof-centric compliance model that is consistent with OFAC's risk-based expectations for the virtual currency sector.

The same pattern is validated in Indicio's ICAO Digital Travel Credential deployments, where passport chip data is verified once and issued as a Verifiable Credential that can be reused across checkpoints and, where permitted, for payments onboarding and remittances. Each presentation is cryptographically verifiable, so participating institutions can run AML and sanctions screening against trusted, government-derived identity data while reducing redundancy, cost, and exposure of raw PII.

Indicio's software platform and infrastructure also supports the assignment of verifiable identities for individuals accessing AI agents and bots, allowing them to authenticate each other and interact within compliance frameworks. This prevents spoofed or malicious automated agents from impersonating trusted entities in financial or customer-facing systems, a growing concern as AI becomes integrated into customer service and transaction processing. Each AI agent can carry a verifiable digital identity credential, enabling least-privilege access and generating immutable, auditable logs of all interactions.

By linking strong identity assurance, cryptographic verification, and interoperability across jurisdictions, with portable verifiable digital credentials, Verifiable Credentials provide the digital asset sector with a practical, standards-based way to mitigate illicit finance risks. Financial institutions using these systems can effectively identify suspicious patterns more effectively, exchange verified identity proofs without revealing sensitive personal data, and maintain continuous compliance in near real time. This approach enhances AML and CFT outcomes and helps digital asset firms meet regulatory expectations for accountability, privacy protection, and global interoperability.

(4a) This section addresses the factors financial institutions consider when deciding whether to employ digital identity verification for AML/CFT and sanctions compliance, the specific compliance functions it supports for those that use or plan to use it, and the rationale of institutions that have chosen not to adopt digital identity verification at this time.

When financial institutions evaluate whether to employ digital identity verification for AML, CFT, and sanctions compliance, they typically consider five key factors: *assurance level, issuer trust, cross-border recognition, privacy impact, and auditability*. They assess whether a solution aligns with recognized assurance frameworks such as NIST SP 800-63, whether the identity issuers can be independently verified, and whether credentials can be used and recognized across jurisdictions without creating gaps in compliance. Institutions also weigh the privacy footprint, specifically how much personally identifiable information (PII) must be stored or shared, and the system's ability to produce verifiable audit trails for regulators. Together, these considerations determine whether a digital identity system can meet both operational efficiency goals and the evidentiary standards required for AML/CFT programs.

Indicio directly supports these priorities and has experience deploying decentralized identity systems. Indicio Proven is a Verifiable Credential platform that allows financial institutions to issue and verify high-assurance verifiable digital credentials derived directly from trusted sources such as passports, government databases, and bank KYC records. Each credential can be cryptographically verified and bound to a live biometric with a signed liveness receipt, creating an auditable chain of trust that satisfies NIST assurance level requirements.

Because credentials are stored in a user-controlled wallet and presented using selective disclosure, they minimize data exposure while maintaining compliance-grade evidence for regulators. Indicio's software architecture has proven effective in supporting multiple compliance functions, including Customer

Identification Programs (CIP), Know Your Customer (KYC) onboarding, sanctions and geographic screening, ongoing due diligence, travel identity validation (as demonstrated in ICAO Digital Travel Credential pilots), and high-assurance passwordless login for regulated systems. By enabling these functions through portable, interoperable, and auditable credentials, Indicio's technology helps financial institutions meet regulatory obligations more securely and efficiently while reducing the risks associated with centralized data storage and repeated identity verification.

(4b) This section describes how financial institutions are using digital identity verification tools within their AML/CFT and sanctions compliance programs, initially to supplement existing processes and, as confidence grows, to replace legacy methods, and compares their effectiveness with traditional tools in improving accuracy, efficiency, and fraud prevention.

Financial institutions are currently using digital identity verification tools primarily to augment existing KYC and AML workflows, with a gradual shift toward replacing legacy processes once Verifiable Credential systems have demonstrated reliability and are compliant with regulatory standards. In early stages, digital identity solutions operate in parallel with traditional document-based methods, serving as an added layer of assurance that validates document authenticity, performs biometric liveness checks, and uses cryptographic signatures to confirm data integrity. As these systems mature and institutions gain confidence in their accuracy and auditability, institutions using Verifiable Credentials begin to replace repetitive and manual document submission processes enabling faster onboarding, cross-platform interoperability, and real-time verification of customer identity. The end goal is to create a continuous, verifiable trust layer that improves compliance efficiency and strengthens defenses against synthetic identity, account take over and cross-border fraud.

An equally important advancement is that digital identity verification provides mutual authentication. Customers can verify that they are interacting with legitimate financial institutions or authorized representatives before sharing sensitive information or approving a transaction. This capability helps eliminate spoofing, phishing, and impersonation scams that are increasingly common in both banking and digital asset markets.

Indicio's deployments demonstrate that integrating Verifiable Credentials with its Indicio Proven® platform allows financial institutions to modernize compliance without disrupting existing infrastructure. Proven connects directly with current AML and identity verification systems and sanctions-screening engines through APIs, for individuals and institutions using Verifiable Credentials to present verified identity attributes, document validation results, and biometric liveness receipts as trusted data inputs. This integration enables institutions to automate identity validation and sanctions checks with higher accuracy, improving monitoring tools that traditionally rely on static or outdated information.

Over time, as institutions measure improved match rates, fewer false positives, and faster onboarding times, many begin phasing out legacy document management systems altogether. Indicio's clients have found that reusable Verifiable Credentials, anchored to authenticated biometrics and document verification, outperform legacy methods by reducing repetitive verification steps, strengthening audit trails, and improving the overall precision of AML/CFT and sanctions compliance programs.

(4c) This section identifies the regulatory, legislative, supervisory, and operational obstacles that hinder the use of digital identity verification to detect illicit finance and mitigate risks involving digital assets, and provides recommendations to address these challenges.

Financial institutions face several regulatory and operational obstacles when adopting digital identity verification for AML/CFT and sanctions compliance, particularly when those systems rely on portable, user-controlled credentials. The most significant challenge is the inconsistent regulatory acceptance of decentralized identity models across jurisdictions and supervisory bodies.

While many regulators recognize the potential of digital identity to enhance security and efficiency, guidance on how portable, Verifiable Credentials fit within existing recordkeeping, audit, and data retention requirements remains limited, restricting industry adoption at scale. Given the nature of the technology, which creates increasing marginal returns at scale, this lack of regulatory clarity is unnecessarily restrictive.

Another barrier is the lack of clarity with regards to selective disclosure policy, a privacy-preserving feature that allows individuals to share only specific, verified data points rather than full identity documents. (*e.g. proving someone is above a certain age without revealing their exact birthdate*)

Institutions lack official guidance whether these minimal disclosures provide sufficient evidence for compliance examinations, since most existing frameworks assume centralized storage of raw KYC data.

Indicio's experience working with financial institutions, governments, and private businesses demonstrates that these challenges can be addressed through clear regulatory positions on standards-based governance and technical proofs. In an environment with clear regulatory positions on the use of digital identity, selective disclosure, and best governance and technical practices, digital identity technologies can play a major role in the detection and mitigation of illicit finance in the digital asset space, by enabling institutions to retain cryptographic proofs of verification (such as digital signatures, issuer attestations, and liveness receipts) across the ecosystem.

To support broader adoption, Indicio recommends that the U.S. Treasury provide explicit regulatory clarification that retaining verifiable proofs (for example, credential hashes or signed attestations) can meet AML/CFT recordkeeping obligations without requiring storage of full identity documents.

Treasury could also promote cross-agency consistency by developing model technical profiles aligned with NIST SP 800-63 assurance levels and FATF digital ID guidance, ensuring that portable digital credentials are accepted as valid, auditable evidence across both domestic and international compliance regimes.

(4d) This section outlines the steps the U.S. government should take to facilitate the effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets.

The U.S. government should make it easier for banks to use digital identity by publishing clear, AML-grade technical profiles for Verifiable Credential issuance and presentation, referencing FATF digital ID guidance, mapping those profiles to NIST assurance levels, and spelling out how VC-based flows satisfy OFAC screening expectations. That clarity should be paired with supervised pilots and conformance testing so institutions can prove outcomes against audit standards without guessing.

Treasury can also provide explicit guidance that the retention of cryptographic proofs (issuer signatures, liveness receipts, credential type) meet recordkeeping requirements without warehousing raw PII.

Finally, Treasury should consider funding cross-sector pilots that link ICAO DTC-derived credentials to payments onboarding and cross-border remittances, as well as publishing shared metrics for effectiveness and privacy and creating a safe path for adoption through examiner playbooks and sample exam artifacts. The international travel industry has addressed similar challenges regarding the incorporation of digital identity into their sector and created international standards of interoperability in order to do so. As a similarly multi-national industry, the financial industry, particularly regulators addressing the growing use of digital assets, would benefit from the technological and governance learnings of that sister industry.

Indicio can help make this real. With the Indicio Proven software platform, we issue and verify high-assurance Verifiable Credentials bound to authenticated biometrics and supported by signed liveness receipts and document chip checks, then pass those proofs to sanctions and AML systems through APIs.

In digital travel, Indicio has implemented ICAO-aligned Digital Travel Credential workflows where passport chip data is verified once, turned into a digital version of a passport, and reused as a portable Verifiable Credential which can then be presented to immigration and border authorities. This same credential could also be presented to financial institutions for onboarding with stronger sanctions screening and less data duplication.

The approach works for banks and fintechs: start by augmenting legacy KYC with Verifiable Credential presentations and signed evidence, measure lower false positives and faster reviews, then progress to partial replacement once controls and audits pass.

If the Treasury sets the technical profiles and acceptance criteria, programs like these can scale nationally with consistent supervision, lower privacy risk, and better illicit-finance outcomes.

(4e) This section provides information relevant to Treasury's evaluation of digital identity verification and its impact based on the research factors identified in the GENIUS Act.

Evaluating digital identity verification through the GENIUS Act framework highlights how portable, verifiable identity systems can enhance AML/CFT programs by improving effectiveness, efficiency, privacy, cybersecurity, explainability, equity, interoperability, and scalability.

Verifiable Credential–based digital identity directly supports these objectives by increasing the accuracy of illicit activity detection, reducing operational costs, strengthening cybersecurity, and improving audit transparency. By adopting these systems, financial institutions can achieve real-time compliance while protecting customer data and reinforcing trust across the digital asset ecosystem.

1. GENIUS Act framework: Effectiveness

Digital identity verification systems built on Verifiable Credentials deliver measurable gains in the accuracy and reliability of AML/CFT programs. Each credential is cryptographically bound to authenticated biometrics and backed by signed evidence such as chip authentication, liveness receipts, and issuer signatures. This provides institutions with a trusted, tamper-evident source of identity information that can be instantly validated.

By aligning credential issuance and presentation with NIST SP 800-63-4 assurance levels, financial institutions can benchmark performance and demonstrate measurable compliance effectiveness across vendors and use

cases. The result is greater transparency and consistency for regulators and auditors, and stronger defenses against fraud, account takeover, and synthetic identity schemes.

2. GENIUS Act framework: Efficiency and Cost Reduction

Reusable digital credentials significantly reduce the operational burden and expense of repetitive KYC processes. Instead of verifying identity data multiple times across accounts or business lines, a single high-assurance credential can be securely presented and verified in seconds. This reduces per-customer onboarding costs, manual review workloads, and human error.

Because Indicio's Proven® platform and similar systems are API-driven, institutions can integrate digital identity verification incrementally into existing AML and sanctions tools. This gradual adoption avoids the high cost and business disruption associated with replacing legacy infrastructure, while enabling continuous improvement of compliance workflows.

3. GENIUS Act framework: Privacy and Cybersecurity

Privacy protection and data minimization are core advantages of decentralized digital identity systems. Using selective disclosure and on-device wallet storage, users maintain control over their personal and biometric data, which is not stored or transmitted through centralized databases. Institutions retain only verifiable proofs. These cryptographic attestations confirm verification results without exposing raw data.

This structure aligns with the FATF's risk-based guidance for digital ID in customer due diligence and minimizes exposure to large-scale breaches, insider threats, and data misuse. The result is a more resilient and privacy-preserving compliance framework that still satisfies regulatory recordkeeping obligations.

4. GENIUS Act framework: Explainability and Auditability

Every Verifiable Credential contains metadata that identifies the issuer, what was verified, and when. These signed proofs can be used to retain clear, immutable audit trails that regulators can easily review. Because all verifications and presentations are cryptographically signed, institutions can produce definitive evidence of compliance actions thus reducing ambiguity and improving audit readiness.

This level of explainability enhances regulator trust and helps institutions defend compliance decisions with verifiable, time-stamped records rather than screenshots or manual attestations.

5. GENIUS Act framework: Equity and Accessibility

Verifiable Credentials promote equitable financial access by allowing individuals to control their credentials and present them across institutions without repeated verification. This benefits individuals who may lack access to traditional banking or in-person KYC processes, such as those in remote or cross-border environments.

By reducing friction in account creation and digital onboarding, verifiable identity tools make compliance-inclusive rather than exclusionary, supporting financial inclusion goals while maintaining rigorous AML standards.

6. GENIUS Act framework: Interoperability and Scalability

Built on open standards referencing both NIST and FATF frameworks, Verifiable Credentials enable interoperability across financial institutions, regulators, and sectors. These systems support a variety of credential formats and protocols that can work globally across jurisdictions, reducing fragmentation and improving data consistency.

Indicio's architecture has proven interoperable across finance, travel, and border management sectors including the eIDAS 2.0 and EUDI framework demonstrating its ability to scale internationally. This standardization supports risk-based supervision and facilitates cross-border regulatory cooperation.

Recommendations

Indicio recommends that the U.S. Department of the Treasury takes the following steps to accelerate the safe and effective adoption of digital identity verification for AML/CFT and sanctions compliance, particularly in the context of digital assets.

1. Publish technical guidance aligning Verifiable Credential use with existing AML/CFT frameworks.

Treasury should issue clear, technical guidance describing how Verifiable Credential–based identity verification satisfies AML, CFT, and OFAC recordkeeping obligations. This guidance should explicitly recognize cryptographic proofs (issuer signatures, credential hashes, and liveness receipts) as compliant evidence of identity verification. By defining these proofs as acceptable substitutes for full PII retention, Treasury would give financial institutions a clear path to modernize compliance without introducing privacy or security risks.

2. Establish model technical profiles and conformance criteria.

Treasury, in coordination with NIST and FinCEN, should develop model technical profiles for Verifiable Credential issuance, presentation, and verification that map directly to NIST SP 800-63 assurance levels and FATF digital ID guidance. These profiles would set consistent expectations for performance, auditability, and interoperability, helping institutions prove compliance to examiners and supervisors. Treasury should also support a conformance testing program—similar to NIST's National Voluntary Laboratory Accreditation Program (NVLAP)—to verify that digital identity systems meet these profiles before deployment.

3. Provide explicit regulatory clarity on selective disclosure.

Treasury should clarify that selective disclosure—allowing an individual to share verified data elements without exposing full identity documents—meets AML/CFT evidentiary requirements when supported by verifiable cryptographic proofs. This would remove a key barrier preventing financial institutions from adopting privacy-preserving technologies and enable the use of Verifiable Credentials at scale while maintaining compliance integrity.

4. Fund supervised pilots to evaluate and demonstrate results.

Treasury should partner with financial institutions and technology providers to launch supervised pilot programs that test Verifiable Credential–based identity verification under real compliance conditions. These pilots should include metrics for fraud reduction, audit readiness, privacy impact, and operational efficiency. Treasury could build on successful international precedents—such as ICAO's Digital Travel Credential pilots—to demonstrate how credential reuse across sectors (e.g., travel, remittances, and digital asset onboarding) improves both compliance outcomes and user experience.

5. Create examiner playbooks and standardized audit artifacts.

To ensure consistent oversight, Treasury should publish sample audit templates and examiner playbooks that describe how regulators can assess identity verification systems based on verifiable proofs. This will help reduce uncertainty during regulatory reviews and accelerate examiner familiarity with new technologies, providing a practical bridge between innovation and supervision.

6. Encourage cross-sector interoperability and international alignment.

Treasury should coordinate with international standard bodies—including FATF, ICAO, ISO, and the European Commission—to align technical definitions and governance frameworks for portable digital identity credentials. Establishing international interoperability will strengthen cross-border AML/CFT efforts and prevent jurisdictional gaps that can be exploited for illicit finance.

7. Leverage lessons from digital travel and identity assurance pilots.

Treasury can draw from existing success in the travel sector, where ICAO-aligned Digital Travel Credentials (DTCs) have demonstrated secure, reusable identity verification between governments, airports, and financial institutions. These programs show how verifiable credentials derived from trusted sources, such as eMRTDs, can be reused for AML onboarding and sanctions screening while reducing redundancy and protecting privacy. Treasury could incorporate similar governance and assurance models into financial compliance frameworks.

8. Promote public-private collaboration on governance and scalability.

Finally, Treasury should establish an advisory working group of financial institutions, regulators, and digital identity experts to guide the development of shared governance principles for Verifiable Credential–based identity systems. This collaboration would support transparent, standards-based deployment across both traditional and digital asset markets and help identify emerging risks early.

Conclusion

Indicio appreciates Treasury's leadership in examining how digital identity can strengthen the integrity of financial systems and reduce illicit finance risk in the digital asset sector. Our experience shows that portable, verifiable identity built on open standards provides a secure, privacy-preserving foundation for compliance. Verifiable Credentials, anchored in authenticated documents, biometrics, and cryptographic proofs, enhance assurance and auditability while supporting interoperability across institutions and jurisdictions.

To advance this opportunity, Indicio respectfully recommends that Treasury:

1. **Publish technical guidance** recognizing cryptographic proofs as compliant evidence under AML/CFT and OFAC frameworks.
2. **Develop model technical profiles and conformance criteria** aligned with NIST SP 800-63 and FATF digital ID guidance.
3. **Clarify the use of selective disclosure** as an acceptable method of verified data exchange.
4. **Support supervised pilot programs** to demonstrate outcomes for fraud reduction, auditability, and privacy protection.
5. **Provide examiner playbooks** and standardized audit templates to ensure consistency and regulatory confidence.
6. **Promote standards-bodies coordination** with FATF, ICAO, ISO, and the European Commission to strengthen interoperability.
7. **Adapt proven lessons** from digital travel credentials to guide governance and assurance frameworks for finance.
8. **Convene a public–private advisory group** to support effective governance and implementation at scale.

Taken together, these steps would provide clarity, encourage innovation, and ensure that digital identity verification contributes to Treasury's goals of secure, risk-based, and privacy-enhancing financial compliance. Indicio welcomes the opportunity to support this work through continued collaboration and shared technical expertise.

###