



**DRC Response to U.S. Treasury RFC: TREAS-DO-2025-0070-0001**  
***Request for Comment on Innovative Methods to***  
***Detect Illicit Activity Involving Digital Assets***

**Submitted by:** Decentralization Research Center (DRC)

**Submission Date:** October 17, 2025

**Executive Summary**

The Decentralization Research Center (DRC) is a 501(c)(4) social welfare think tank focused on ensuring that the future of digital infrastructure is decentralized, privacy-preserving, and aligned with democratic values. We advocate for regulatory frameworks that promote resilient, censorship-resistant systems where users control their own identity and data, rather than intermediaries.

This submission responds to the Treasury's request for comment with the goal of shaping the dialogue around compliance in the digital asset ecosystem. We offer a vision of compliance that:

1. Avoids the harms and shortcomings of legacy systems - including those that rely on bulk data collection, retrospective surveillance, and centralized chokepoints - which have failed to meaningfully reduce illicit finance and often infringe on civil liberties.
2. Emphasizes decentralization as a feature that strengthens consumer protection and reduces illicit finance risks by increasing transparency, limiting single points of failure, and enabling open auditability.
3. Aligns AML/CFT outcomes with civil liberties.

Treasury should resist the temptation to retrofit legacy frameworks onto public blockchains and instead look to the native attributes of decentralized, cryptographically secure architectures. These tools can protect civil liberties while enhancing compliance integrity by minimizing honeypots, chokepoints, and governance opacity.

Privacy is a fundamental right, not a regulatory constraint, and systems should be built around purpose limitation, data minimization, and user agency. Frameworks need to move toward open, verifiable, and decentralized governance models where compliance can be proven cryptographically rather than trusted institutionally. In short, what's needed is a shift from compliance through control to compliance through verifiability - grounded in dignity, accountability, and open governance - where detection itself is based on cryptographic proof of anomalous behavior, not identity correlation or dragnet surveillance.

Our recommendations align with emerging academic frameworks for compliance-compatible identity systems, particularly the Compliance SSI System Property Set (CSSPS) developed by

Pattiyanon & Aoki (2023), which defines system properties reconciling decentralized identity with international privacy law and regulatory requirements.

History demonstrates that surveillance capabilities built for narrow purposes inevitably expand beyond their original scope. Architectural choices made today will shape privacy and civil liberties for decades, making principle-based design essential.

## Q1.

### **What are the most important recent trends or developments in detecting illicit finance involving digital assets?**

The most important development is the maturation of privacy-preserving compliance primitives built atop decentralized architectures. These include:

- Selective disclosure using zero-knowledge proofs (ZKPs)
- User-held, verifiable digital credentials (VDCs)
- Identifiers controlled by users, such as blockchain accounts and Decentralized Identifiers (DIDs)
- Multi-party computation and threshold-based decryption for lawful access

These technologies allow institutions to verify facts (e.g., "not on sanctions list") without collecting or storing personal data. Critical to their deployment are device-binding mechanisms and interactive verification protocols that prevent credential transferability or resale, ensuring that verifiable credentials cannot be copied or transferred between users.

At the same time, efforts to apply traditional compliance tools, such as retroactive blockchain surveillance or centralized identity gatekeepers, are increasingly ineffective, especially with the emergence of privacy-preserving chains (e.g., shielded L2s, encrypted rollups, FHE-native networks). These developments weaken the utility of retroactive surveillance and underscore the need to shift toward verifiable, consent-based systems designed around privacy. Traditional approaches not only fall short in this evolving context, they also carry significant downsides:

- They recentralize infrastructure, creating single points of failure and harmful surveillance
- They exclude lawful users, particularly in marginalized populations, due to high onboarding burdens
- They generally fail at enforcement, with very low interception rates for illicit flows
- They fail to address cross-chain flows, which represent the primary vector for illicit finance in practice today

**Implementation Pathway:** Treasury should initiate pilot programs with NIST and private sector actors to test privacy-preserving compliance protocols on open blockchain networks, focusing on zero-knowledge verification of sanctions compliance and age/ID eligibility.

**Q4.**

**How can digital identity verification be improved in a manner that supports both financial integrity and civil liberties?**

Modern identity systems must be built on six core pillars:

1. **Data Minimization:** Only disclose what is strictly necessary
2. **User Control:** Users must hold and manage their own credentials
3. **Open Standards:** Systems should be built using open and widely available standards such as W3C Verifiable Credentials and DIDs
4. **No Mandatory Intermediaries:** Users must be able to prove eligibility without being required to go through centralized brokers. Users should be free to choose intermediaries if they want one, but systems must not hardcode their use. Where access is required, it should be based on auditable proofs of attributes, not full identities.
5. **Voluntary Adoption:** Digital identity systems must remain optional. Users must retain the right to complete compliance through traditional paper-based methods without penalty or discrimination
6. **Purpose Limitation:** Identity data must only be usable for its intended function, with strong technical and legal enforcement

These principles contrast sharply with today's KYC regime, where individuals routinely surrender complete personal dossiers to every financial service they use, resulting in duplicated exposure and systemic surveillance risk.

**Implementation Pathway:** Treasury should adopt a regulatory position that verifiable digital credentials (VDCs) from qualified issuers are sufficient for Customer Identification Program (CIP) purposes, especially when paired with zero-knowledge attestations.

**Q5.**

**What role can blockchains or blockchain analytics play in identifying and disrupting illicit finance?**

Blockchains provide the opportunity for transparency without surveillance. Their public, tamper-resistant nature enables auditability through cryptographic proof rather than data collection.

Beyond transparency, blockchains provide verifiable governance infrastructure through cryptographic voting, attestation registries, and decentralized oversight mechanisms. These enable compliance coordination without creating new centralized chokepoints - a model that should inform how Treasury thinks about accountability architecture.

However, blockchain analytics tools, as currently deployed, often attempt to map pseudonymous activity to real-world identities via off-chain surveillance or heuristics, undermining privacy and increasing discriminatory bias.

Instead of mass deanonymization, Treasury should support event-based, consent-driven analytics that:

- Focus on network risk patterns, not individual identity
- Respect on-chain pseudonymity by default
- Use selective proof frameworks (e.g., ZK compliance attestations)

**Implementation Pathway:** Treasury should actively engage with independent blockchain forensics and monitoring communities such as the Security Alliance (SEAL), which conduct high-quality, public-interest transaction analysis. In our experience at DRC, these experts are not only effective at identifying illicit behavior but also serve as stewards of ecosystem integrity. Most builders and analysts in decentralized systems are proactive, cooperative, and mission-aligned with the government's goals. Yet, they often operate without public support and face elevated personal risk due to overly broad enforcement tactics. Rather than treat these actors as adversaries, Treasury should view them as valuable allies and build structured, ongoing engagement pathways. Treasury can partner with these open-source communities to fund privacy-preserving analytics libraries that support AML signal detection without needing to unmask identities by default.

## Q6.

### **What other emerging technologies may be relevant for detecting or mitigating illicit finance risks involving digital assets?**

Emerging technologies, especially those native to the blockchain ecosystem, now offer the unprecedented ability to detect risk, prove compliance, and preserve civil liberties, all at once. These technologies should not be viewed narrowly as confidentiality tools but rather as infrastructure for provable, verifiable compliance and collaborative enforcement. When integrated properly, they empower regulators and technologists alike to advance shared goals: reducing illicit finance without sacrificing human rights.

For instance, zero-knowledge proofs and MPC can demonstrate compliance without revealing sensitive data; trusted hardware can generate device-level attestations that prove policy adherence; and fully homomorphic encryption enables encrypted auditability. These technologies are not just privacy-preserving, they enable compliance and collaborative enforcement by design.

- **Zero-Knowledge Proofs (ZKPs):** Prove "yes/no" answers to compliance checks without exposing underlying data

- **Multi-Party Computation (MPC):** Enable collaborative sanctions screening, risk scoring, and transaction analysis without any party revealing underlying data. MPC already forms the technical backbone of large-scale privacy-preserving identity systems in production and directly achieves data minimization principles
- **User-controlled identifiers:** such as decentralized identifiers (DIDs) or blockchain-native addresses, enable user control over identity data and allows key facts to be proven without relying on centralized authorities
- **Privacy-Preserving Credential Frameworks:** Combine auditability with selective disclosure
- **Threshold Encryption and Secure Multi-Party Access:** Provide verifiable, lawful access to sensitive data only with appropriate oversight and cryptographic distribution of authority
- **Trusted Hardware for Secure Attestations (e.g., TEEs):** Enable devices to generate verifiable, tamper-resistant compliance proofs
- **Fully Homomorphic Encryption (FHE, early-stage):** Allow computations on encrypted transaction data for anomaly detection, enabling scans for illicit patterns without decryption (i.e., without access to the raw data), which can support capability for DeFi audits and regulatory oversight while preserving data privacy.

Together, these technologies enable Treasury’s objectives - risk detection, credential validation, and behavioral monitoring - without mass data aggregation or retrospective surveillance, enabling provable compliance without compromising user privacy. These systems don’t merely replace existing tools - they redefine how compliance can be achieved without sacrificing privacy or resilience.

**Implementation Pathway:** Treasury should establish a regulatory sandbox or convene a working group composed of privacy engineers, compliance architects, and civil liberties organizations to pilot and evaluate these technologies in practice. Treasury should also issue guidance clarifying that cryptographically verifiable compliance systems, even those that minimize data exposure, may satisfy existing AML/CFT obligations under the Bank Secrecy Act.

### Additional Recommendations

1. **Mandate Purpose Limitation Statutes:** Systems designed for AML/CFT must not be legally usable for other unrelated surveillance or commercial purposes
2. **Exclude Open-Source Builders from AML Burdens:** Clarify that developers of privacy tools are not "financial institutions" for BSA purposes
3. **Fund Open Compliance Infrastructure:** Use public funds to support open-source, verifiable credential and ZK toolkits
4. **Elevate Decentralization in Risk Scoring:** Decentralized architectures reduce systemic risk and must be viewed as a regulatory positive

5. **Prioritize Financial Inclusion in Design:** Compliance systems must be evaluated for accessibility to unbanked and underbanked populations, with explicit prohibitions on discriminatory denial and cost structures that don't create new barriers to access
6. **Apply Antitrust Scrutiny to Identity Infrastructure:** Prevent market consolidation that could create monopolistic control over compliance infrastructure, ensuring competitive markets for credential issuers, wallet providers, and verification services
7. **Prepare for Delegated and Agent-Based Identity:** As AI agents gain the ability to hold keys and initiate transactions, Treasury must develop frameworks for delegated credentials, derived attestations, and auditable authorization scopes that maintain accountability when the "customer" is not a human end-user

**Evaluation Criteria for Proposed Systems:** Treasury should assess compliance architectures using standardized criteria including: (1) data minimization enforcement, (2) decentralization of control over both the verifiable data and the systems that generate it, supported by open standards that enable a competitive ecosystem rather than reliance on a single gatekeeper, (3) technical purpose limitation, (4) financial inclusion impact, and (5) standards-based maturity. Systems should be scored transparently against these dimensions.

**Implementation Pathway:** Use evaluation criteria as outlined above. Include "level of decentralization" as a factor in FinCEN guidance on evaluating compliance architectures, with reference to open-source standards and governance diversity.

We thank you for the opportunity to submit this comment.

Sincerely,  
Decentralization Research Center (DRC)

### **Acknowledgments**

This submission benefited from technical review and substantive input from experts in privacy-preserving identity systems, cryptographic protocols, and decentralized governance. They include Aisling Connolly (TACEO), Kim Hamilton Duffy (Decentralized Identity Foundation), Mike Norman (Consensys), and Wayne Chang (SpruceID). We are grateful for their insights on compliance architectures, multi-party computation, and verifiable credential standards.

The views and recommendations expressed herein represent the institutional position of the Decentralization Research Center.