VIA REGULATIONS.GOV

October 17, 2025

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

RE: Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, Document Number–2025-15697

The Crypto Council for Innovation ("CCI") appreciates the opportunity to submit comments on the U.S. Department of the Treasury's Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets (the "RFC").

By way of background, CCI is a global alliance of industry leaders in the digital assets space with a mission to communicate the benefits of digital assets and demonstrate their transformational promise. CCI members span the digital asset ecosystem and share the goal of encouraging the responsible global regulation of digital assets to unlock economic potential, improve lives, foster financial inclusion, protect national security, and disrupt illicit activity. CCI believes that achieving these goals requires informed, evidence-based policy decisions realized through collaborative engagement. To that end, CCI provides our comments and recommendations to the RFC, responding to questions 1, 3, 4, 5, and 6.

1. *In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem? What key trends in illicit finance risks have financial institutions observed in the digital asset ecosystem?*

Several key illicit finance risks and vulnerabilities represent certain significant threats in the digital asset ecosystem. Understanding these risks requires distinguishing among different types of security vulnerabilities across centralized exchanges, decentralized finance (DeFi) protocols, and underlying blockchain infrastructure.

Cyberhacks and Theft. Cyber intrusions represent a major category of risk, particularly those linked to North Korea-related activity. These exploits primarily stem from vulnerabilities in cybersecurity practices of centralized platforms rather than fundamental flaws in the underlying blockchain protocols. The industry participants are responding through coordinated

information-sharing through initiatives such as the SEAL Alliance,[1] Crypto-ISAC,[2] and IVAN,[3] which facilitate real-time threat intelligence exchange among digital asset institutions and support communication with law enforcement.

Scams and Social Engineering Fraud. Pig butchering and related schemes account for substantial consumer losses. Much of the associated money laundering and cash-out activity occurs through non-compliant exchanges operating outside U.S. jurisdiction. Industry efforts to counter this include comprehensive scam prevention awareness campaigns and collaborative resources to flag illicit wallets, such as the Chain Abuse website,[4] which represents a partnership among many digital asset institutions to share threat intelligence.

Non Compliant Crypto Kiosks. Criminal exploitation of certain non-compliant crypto kiosks has increased, especially in connection with scams and street-level crime activity. While these businesses are covered under the Bank Secrecy Act (BSA), many operators fail to implement effective Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) controls, creating exploitable gaps, as mentioned in FinCEN's August 2025 advisory.[5]

Global Regulatory Arbitrage. Criminals continue to exploit jurisdictions with inadequate AML/CFT frameworks. The Financial Action Task Force's 2025 update[6] on virtual asset supervision highlights the uneven global implementation of anti-money laundering standards, with many jurisdictions lacking proper registration and licensing regimes for the digital asset—creating opportunities for regulatory arbitrage that sophisticated criminal networks exploit.

2. *[NO RESPONSE]*

3. *What innovative or novel methods, techniques, or strategies related to AI are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to AI? Please describe the use of AI to conduct analysis of transactional data, including transactions that occur on blockchains, and to identify complex illicit financial networks, as well as key lessons learned from use of AI in this context.*

Financial institutions are deploying AI technologies in increasingly sophisticated ways to detect illicit activity and mitigate illicit finance risks involving digital assets. The use of AI in this

[1] https://www.securityalliance.org/
[2] https://www.cryptoisac.org/
[3] https://www.mitre.org/news-insights/news-release/illicit-virtual-asset-notification-public-private-partnership
[4] https://chainabuse.com/
[5] https://www.fincen.gov/system/files/2025-08/FinCEN-Notice-CVCKIOSK.pdf
[6] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

context delivers major benefits but also raises unique governance challenges that require careful consideration.

AI for Pattern and Anomaly Detection. Financial institutions are utilizing AI for advanced signals and pattern detection, combining on-chain transaction data with off-chain information—device data, login patterns, and behavioral analytics—to detect anomalies at scale. These AI systems can identify suspicious patterns that might be difficult for human analysts to detect, particularly when dealing with large volumes of transaction data across multiple blockchain networks.

AI Assistants in Compliance Operations. AI assistants are increasingly being deployed to support compliance investigations, helping analysts summarize customer and transaction data, synthesize complex information, provide high-level investigation setup details, and gather relevant internet research. This frees up investigators' time, allowing them to focus more attention on judgment-based decisions (and less on repetitive research tasks). The use of AI tools within compliance operations is largely focused on streamlining routine tasks while ensuring that critical decision-making remains under human oversight.

AI for Cyber Reliance. Given the immutable nature of digital asset transactions, certain breaches and hacks on crypto exchanges can result in irreversible losses, making proactive security measures essential. AI technologies can stress-test smart contracts before deployment, identify vulnerabilities, and continuously scan for anomalous code behavior.

Companies such as OpenZeppelin,[7] ChainPatrol,[8] and CertiK[9] are already utilizing AI to analyze historical blockchain data and detect fraudulent activity, enhancing the security and reliability of digital payment systems. For example, Blowfish, a crypto wallet security solution proactively inhibits fraudulent transactions in real time by incorporating machine learning algorithms to identify patterns indicating that wallets may be interacting with a scam website.[10] AI tools make this process significantly more efficient and comprehensive.

Blockchain Analytics and Attribution. Blockchain analytics firms utilize AI and machine learning for fraud and risk detection in on-chain activity, enabling platforms to flag and mitigate illicit activity in real-time. AI-powered attribution systems can help identify wallet ownership patterns and transaction relationships that might indicate illicit activity, though distinction between AI-generated attribution and human-generated attribution remains an important consideration for accuracy and reliability.

[7] https://www.openzeppelin.com/
[8] https://chainpatrol.com/
[9] https://www.certik.com/
[10] https://gen.xyz/blog/blowfishxyz

(a) What factors do financial institutions consider when deciding whether to employ AI for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use AI for these purposes, what specific compliance functions does/will AI support? For financial institutions that decided not to use AI, please provide additional details on the rationale for that decision.

Financial institutions consider several factors when deciding whether to employ AI for AML/CFT and sanctions compliance purposes. In evaluating eligible processes, institutions prioritize tasks that are repeatable, consistent, and capable of ongoing testing and validation. AI is generally applied to augment, not replace, human reviewers. Most financial institutions are generally in the early stages of adopting AI tools for compliance review processes, with the expectations that AI tools will improve efficiency and accuracy over time.

(b) How are financial institutions using AI tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of AI tools with other previous or existing tools used for similar purposes.

Institutions are using AI to augment existing compliance tools rather than supplant legacy monitoring systems. AI technologies are typically deployed in testing phases alongside existing systems, allowing institutions to benchmark results and document governance controls before broader implementation. The overarching objective is to enhance human capabilities, not substitute human judgment in critical compliance decisions.

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using AI to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Some BSA-covered financial institutions remain hesitant to integrate AI into compliance operations due to the absence of explicit supervisory guidance confirming that such use will not negatively affect an institution's regulatory standing. The challenge is that certain regulatory governance expectations—such as rigorous governance and explainability—can sometimes result in slower iteration on AI-based controls, making it difficult to keep pace with rapidly evolving risks involving digital assets.

This challenge mirrors earlier uncertainty around statistical models before standardized Model Risk Management (MRM) standards were established with general acceptance across industries. Given the historically deliberate pace of AML regulatory guidance, industry remains concerned about delayed clarity on AI usage.

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

Treasury and FinCEN should consider providing clear guidance on permissible AI uses in compliance contexts, emphasizing risk-based flexibility rather than prescriptive rules. Guidance should balance the need for governance and explainability with the practical requirements for keeping pace with evolving digital asset risks. Additionally, government agencies should consider leveraging AI technologies to improve sanctions-enforcement analytics and suspicious-activity triage, thereby enhancing their overall supervisory and sanctions enforcement capabilities.

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? What are the risks, benefits, challenges, and potential safeguards related to digital identity verification? Please describe the portable digital identity credentialing tools in use and how such tools are being used.*

Digital identity solutions, particularly those utilizing decentralized technologies, offer significant opportunities to enable more secure and efficient forms of identity verification for AML/CFT compliance. In addition, these technologies are especially valuable for DeFi risk management applications where traditional centralized identity verification methods may be less practical.

Decentralized ID (DID). DID provides an innovative approach to Know Your Customer (KYC), sanctions screening, and credentials verification based on cryptographic proofs rather than redundant uploading of documents. This reduces unnecessary data exposure, disincentivizes the creation of data honeypots that attract cybercriminals, and puts users in greater control of their personal information and how it is shared. Examples of entities developing these solutions include Persona[11] and Z-Pass,[12] among others developing privacy-preserving identity verification systems.

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Current BSA rules constrain customer-onboarding approaches, preventing full realization of decentralized identity benefits unless FinCEN issues guidance confirming and clarifying that DID can be used to support AML/CFT compliance goals.

Financial institutions face a Catch-22 in adopting novel blockchain-based compliance tools. These approaches can help manage illicit finance risks within the very architecture of blockchain systems and reduce unnecessary private data collection, but BSA-covered institutions are unlikely to test and develop them in the absence of official guidance approving such techniques to support AML/CFT compliance goals. Out of all these blockchain-based

[11] https://withpersona.com/
[12] https://zpass.aleo.org/

compliance approaches, approving innovative digital identity solutions should be a key focus of new regulatory guidance.

Decentralized identity and credentials support the goals of the BSA by addressing illicit finance risks while allowing institutions to meet BSA compliance requirements through a more refined approach. A blockchain-based identity credential does not eliminate the KYC framework, but instead limits the collection of documents and verification of their authenticity to a trusted third party separate from the financial institution. In this model, KYC is satisfied through a mathematical proof of document authenticity rather than submission of the document itself.

The use of DID credentials for illicit finance risk management of digital assets in different scopes, depending on whether the platform is a centralized finance (CeFi) or DeFi service. For money service businesses, this would not necessarily require significant changes to the BSA. Rather, it could simply be an option for institutions to accept decentralized credentials to support the current KYC process. For example, when John Smith opens an account at CeFi Exchange A, he could provide his decentralized identity proof to confirm the personal details that the exchange needs to verify rather than uploading his identity documents. This would streamline onboarding and reduce the opportunities for bad actors to present forged documents to exchanges. However, this would not alter the type of information that the exchange needs to collect, record, and share for other regulatory record-keeping or reporting. For instance, when CeFi Exchange A provides John Smith's identification data to CeFi Exchange B in compliance with the travel rule,[13] it would still transmit the same required KYC information whether it was verified with or without DID credentials.

However, in a fully decentralized service, with no intermediary controlling user funds or able to collect and verify KYC data, DID credentials could be useful through smart contracts to mitigate the risks of illicit funds entering the platform. For example, a DeFi service could be designed or augmented to enable users to share verified credentials that confirm that the wallet holder is not on a sanctions list or to confirm other details such as citizenship or country of residence, without revealing the user's precise identity or other personal information. This type of approach to illicit finance mitigation is discussed further below for the response to question 6.

In order to consider more innovative KYC practices for regulated financial institutions, it is important to clarify how identity verification operates under the BSA. The United States currently operates under a two-pillar approach to Customer Identification Programs (CIP): Collect and Verify. Most major countries outside the United States have evolved to a three-pillar approach: Collect, Verify, and Corroborate. The corroboration element, which addresses the strength and degree of separation between the client providing information and the financial

[13] https://www.fincen.gov/system/files/advisory/advissu7.pdf

institution, needs to be more clearly delineated in U.S. regulatory frameworks. Corroboration speaks to the degree of a client's inability to alter or tamper with information accuracy and typically involves sources that have conducted some level of validation.

When considering recent regulatory guidance such as the CIP TIN collection exemption, it would be beneficial to include decentralized identity within the scope of "alternative collection methods." Broadening the scope of KYC reliance to account for the advances occurring in advanced cryptography and blockchain technology would benefit customers by protecting their data. Financial institutions could collaborate to provide input on verification and accuracy standards for these new approaches.

It also should be noted that decentralized identity and credentials are being piloted for non-financial use cases by various government agencies. For example, SpruceID is working with the Department of Homeland Security in piloting DID for passport entry and citizenship verification[14] and with the State of California for mobile drivers license technology.[15]

(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?

FinCEN has previously conducted Digital Identity sprints and should continue facilitating formal exchanges with industry, especially around decentralized identity methods, which involve unique architectures compared to centralized approaches to data verification and credentialing. FinCEN should publish guidance outlining that decentralized identity approaches can be used to support AML/CFT and sanctions compliance objectives.

Financial institutions could align on standards for reliance on obtaining verification information from alternative sources, which would be particularly helpful if some institutions become issuers of verifiable credentials. This approach could benefit smaller institutions by potentially reducing operational costs associated with verification and data management. Further opportunities could include financial institutions relying upon issuers' verifiable credentials to create consortiums for information sharing purposes.

5. *What innovative or novel methods, techniques, or strategies related to blockchain technology and monitoring are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to blockchain technology and monitoring? Please describe how financial institutions are integrating information from blockchain*

[14] https://www.dhs.gov/science-and-technology/spruceid

[15] https://blog.spruceid.com/state-of-california-department-of-motor-vehicles-open-source-mobile-wallet-for-decentralized-digital-credentials-named-by-gartner-as-2023-innovation-award-winner/

analytics with off-chain data and mention any key challenges associated with using blockchain analytics (e.g., obfuscation tools and methods that can complicate tracing and assessing confidence in attribution or complexities inherent in cluster analysis).

Blockchain analysis tools have become essential components of modern AML/CFT and sanctions compliance programs and continue to evolve beyond basic transaction monitoring capabilities. These tools now offer advanced capabilities for identifying malicious wallets, providing real-time intelligence on critical infrastructure threats, and supporting sophisticated fraud detection efforts.

Modern blockchain analysis tools are expanding their capabilities to include real-time threat detection, advanced pattern recognition, and integration with threat intelligence feeds. Companies like Blockaid[16] and others are developing next-generation tools that can identify emerging threats such as malicious wallets and provide actionable, real-time intelligence to compliance teams.

(b) How are financial institutions using blockchain technology and monitoring tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of blockchain technology and monitoring tools with other existing or previous tools used for similar purposes.

Blockchain analysis tools are essential components of AML/CFT and sanctions compliance for centralized exchanges, stablecoin issuers, and increasingly, some DeFi protocols that incorporate blockchain analytics into their front-end interfaces. Compliance personnel use blockchain forensics software to understand the provenance of wallets interacting with their platforms and to block transactions involving sanctioned addresses. These tools enable clustering and pattern recognition capabilities that help unwind criminal obfuscation methods.

Institutions' compliance and investigation teams rely on blockchain analysis to identify illicit activity occurring on other platforms, enabling them to proactively flag wallets that could potentially interact with their customers in the future. Data from blockchain analysis is often included in Suspicious Activity Reports (SARs), helping law enforcement develop leads for criminal investigations. However, it's important to note that some SAR reporting of on-chain data may be somewhat outdated, as law enforcement agencies should facilitate their own access to the same blockchain information in real-time through their own analytical tools. As FinCEN is currently seeking ways to reduce the burdens and costs driven by inefficient AML/CFT compliance practices,[17] it should consider ways to eliminate the practice of SARs reporting that

[16] https://blockaid.io/

[17] https://www.federalregister.gov/documents/2025/09/30/2025-18918/agency-information-collection-activities-proposed-new-information-collection-survey-of-the-costs-of

simply duplicates transactions that law enforcement clearly can access and identify directly without a SAR.

> *(c) Are there regulatory, legislative, supervisory, or operational obstacles to using blockchain technology and monitoring to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.*

Although covered institutions heavily utilize blockchain forensics software to support compliance functions, the lack of standardization across these tools can lead to discrepancies in wallet attribution and analysis. Some institutions find it challenging to rely more extensively on such tools for compliance purposes without objective quality standards to evaluate software performance. This standardization concern becomes particularly important when blockchain analysis is later used in legal proceedings.

Two specific areas lack clear regulatory guidance:

First, blockchain information continuously updates, and what was reviewed at one point in time may not reflect the same attribution or risk assessment in the future as vendors improve their ability to attribute wallet activity to underlying owners. When examiners review historical decisions, they sometimes question why future-state updates did not prompt some type of feedback loop to the original review, which is not practical as it would require continuous monitoring of all historical transactions. Clear guidance should establish that financial institutions are not expected to conduct continuous post-event monitoring.

Second, guidance should address expectations regarding how many transaction "hops" away from an immediate transaction financial institutions should consider when conducting compliance reviews.

> *(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of blockchain technology and monitoring for detecting illicit finance involving digital assets?*

FinCEN should work collaboratively with the digital asset industry to provide guidance on standards for evaluating blockchain analysis software, including considerations for attribution methodologies and the distinction between AI-generated attribution and human-generated attribution. This can be accomplished as part of the mandatory path outlined in Section 9 of the GENIUS Act, in which FinCEN will "issue public guidance and notice and comment rulemaking" relating to "the implementation of innovative or novel methods, techniques, or strategies by regulated financial institutions to detect illicit activity involving digital assets."[18]

[18] https://www.congress.gov/bill/119th-congress/senate-bill/1582/text

After considering public input from this RFC, Treasury should augment its research on novel and innovative techniques by conducting formal FinCEN Exchange sessions with blockchain analysis firms, centralized exchanges, and other blockchain experts to better understand best practices and technical factors that impact the performance of blockchain analysis tools.

6. *What innovative or novel methods, techniques, or strategies related to any other innovative technologies such as cryptographic protocols and other privacy-enhancing tools, cloud-based solutions, on-chain compliance tools, oracles, or new verification tools for smart contracts are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to these other innovative technologies?*

The digital asset industry is developing and deploying various forms of blockchain-based illicit finance risk management tools that deserve formal consideration as measures to address illicit finance activity. CCI has highlighted several of these tools in its *Crypto Illicit Finance Risk Management Guide*,[19] and these technologies represent significant opportunities for enhancing compliance capabilities while preserving privacy and user control.

The following deserve formal consideration as blockchain-based measures to address illicit finance activity:

- **Zero-Knowledge Proofs** (ZKPs) are cryptographic tools that allow one party to prove knowledge of certain information without revealing the actual information itself. They can verify the validity of transactions or user credentials without disclosing sensitive data, thus preserving user privacy while supporting compliance. For instance, before withdrawing funds from a DeFi service, a digital asset wallet holder could use a ZKP protocol to confirm that the wallet address is not on a sanctions list and has not received funds directly or indirectly from a sanctioned address. ZKPs offer a technical framework for blockchain developers to build checks, screening, and regulatory compliance even into privacy-preserving protocols and services, as discussed in the 2022 a16z white paper on privacy-preserving regulatory solutions.[20]

- **Association Sets** such as "privacy pools"[21] represent novel smart contract-based protocols that allow users to demonstrate regulatory compliance by publishing

[19] https://cryptoforinnovation.org/wp-content/uploads/2024/05/CCI-Crypto-Illicit-Finance-Risk-Management-Guide.pdf?_gl=1*18aoyz*_ga*MTc1MTA2ODc3NC4xNjkyODkwNTIx*_ga_F9NE23R22E*MTcxNTIwMjAxOC4zOTIuMS4xNzE1MjAyNDEwLjkuMC4w

[20] https://a16zcrypto.com/posts/article/privacy-protecting-regulatory-solutions-using-zero-knowledge-proofs-full-paper/#section--11

[21] As suggested by Buterin et al, see: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364

zero-knowledge proofs showing that their funds are not illicit or that they originate from lawful sources without revealing their entire transaction histories. Users could opt-in to have their assets verified through ZKPs to be grouped into a pool of verified non-illicit funds.

- **Token Extensions** help developers build tokens that follow set rules, including for preventing illicit financial flows. Platforms such as Solana's Token Extensions[22] embed compliance capabilities directly into digital asset infrastructure.

- **Pre-Transaction Computation** software enables blockchain applications to operate according to programmable policies, creating the capability to implement transaction-specific policies for smart contracts (such as asset flows to avoid, dynamic inclusion/exclusion lists, etc.) in a decentralized manner. Companies like Predicate[23] are developing these capabilities, as demonstrated in collaborative work with Paxos on Uniswap integration.[24]

- **Attestation Tokens** are cryptographic tools that enable the issuance, verification, and presentation of digital credentials or proofs. These credentials allow users to demonstrate the authenticity of certain attributes or claims without disclosing the underlying data. Attestation tokens would support digital ID infrastructure; a user undergoing KYC to verify identity, reputation, or compliance status would receive credentials at a third-party provider and then acquire attestation tokens to transact on a DeFi platform. The tokens' link to a verified identity would reduce the risk of fraudulent activities and illicit fund flows. Decentralized identity tools further enhance this model by giving wallet holders control over their own data, enabling them to decide what information to disclose and when—thereby maintaining verification integrity while protecting privacy.

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using other innovative technologies to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Currently, the benefits of these innovative tools are either unavailable to institutions or significantly constrained due to rules within the BSA that restrict compliance methods. The lack of regulatory safe harbors for innovative compliance approaches creates uncertainty that discourages adoption. More institutions would utilize these types of tools if there were official guidance allowing greater flexibility in technological approaches to support AML/CFT compliance goals.

[22] https://solana.com/solutions/token-extensions
[23] https://predicate.io/
[24] https://drive.google.com/file/d/1iT0_YPU0v1gbfovzrIn5wDDOsz-EcmDg/view

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

FinCEN should publish guidance confirming that decentralized identity approaches and other privacy-preserving compliance technologies can be used to satisfy AML/CFT and sanctions compliance objectives when properly implemented. Financial institutions can align on common standards for reliance on obtaining verification information from alternative sources, particularly if some institutions serve as verifiable-credentials issuers.

Additionally, Congress should consider allocating funding to fully staff a regulatory digital asset sandbox focused on privacy-preserving compliance solutions. While Treasury may face challenges in supervising such a sandbox, establishing this capability would signal the importance of fostering innovation in compliance technologies.

CCI respectfully also recommends that market structure legislation should establish a safe harbor provision to provide the digital assets industry with additional tools necessary to responsibly combat illicit finance, while encouraging bipartisan support for practical but robust AML/CFT measures. CCI further details specific recommendations below:

The Department of the Treasury,through OFAC and FinCEN, and in coordination with the Department of Justice (DOJ), should develop and implement a formal Safe Harbor program for digital asset services. Participants in the safe harbor should not be held liable in federal or state civil court for actions taken to block / freeze digital assets if conducted in accordance with the safe harbor program, including providing notification to OFAC, FinCEN, and/or DOJ, as appropriate. Treasury should retain discretion to develop and modify the categories of entities eligible for safe harbor and should be permitted through rulemaking to issue guidance around the implementation of the safe harbor program. Such a framework would foster investment in innovative compliance solutions and strengthen deterrence of illicit activity on digital asset platforms.

* * *

Conclusion

The digital asset industry continues to develop innovative solutions to counter illicit finance while preserving the benefits of digital assets for lawful users. Technologies such as AI-driven analytics, decentralized identity, and zero-knowledge proofs offer substantial opportunities to enhance the effectiveness of AML/CFT compliance, lower compliance costs, and enhance user privacy. However, realizing these benefits requires updated regulatory guidance that

acknowledges the unique characteristics of digital assets and provides clear pathways for institutions to adopt innovative compliance approaches.

CCI looks forward to continued collaboration with Treasury and other regulatory agencies to develop frameworks that support both innovation and robust compliance with AML and sanctions requirements.

Respectfully,

Ji Hun Kim
Chief Executive Officer
Crypto Council for Innovation