Chainlink Labs

October 17, 2025
Submitted electronically via regulations.gov

Julie Lascar
Director, Office of Strategic Policy, Terrorist Financing and Financial Crimes
United States Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Re: Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets

Chainlink Labs Inc. ("Chainlink Labs") welcomes the opportunity to respond to the U.S. Department of the Treasury's ("Treasury") request for comment on "Innovative Methods To Detect Illicit Activity Involving Digital Assets" (the "RFC")[1]. As a leader in the digital assets space and a builder of technology infrastructure, Chainlink Labs supports effective, technology-forward regulation developed with input from the industry.

Chainlink Labs is one of the primary contributing developers of Chainlink. Chainlink is the industry-standard oracle platform bringing the capital markets onchain and powering the majority of decentralized finance. The Chainlink stack provides the essential data, interoperability, compliance, and privacy standards needed to power advanced blockchain use cases for institutional tokenized assets, lending, payments, stablecoins, and more.

Our submission is organized around four concepts we believe are most relevant to Treasury's inquiry. Based on our work with financial market infrastructures and financial institutions and our engagement with policy makers, we believe portable digital identity, distinguishing administrative control from customer relationships, rules-based onchain compliance, and cryptographically-assured reserve transparency can materially improve illicit-finance detection while reducing privacy concerns and operational risk.

1. **Portable, privacy-preserving digital identity can improve compliance efficacy while reducing friction**

Current compliance processes rely on siloed compliance systems and expensive onboarding processes, resulting in billions of dollars in redundant onboarding costs for financial institutions that are ultimately passed on to consumers.[2] For example, even if the same institutional client is known to multiple parties in a transaction, each regulated firm often must collect the same sensitive client information in order to verify that client's identity independently. Put simply, financial institutions are faced with a dilemma: they

[1] 90 Fed. Reg. 40148 (Aug. 18, 2025), as directed under Section 9(a) of the GENIUS Act, Public Law 119–27, 139 Stat. 419.
[2] According to research by LexisNexis and Forrester Consulting, the total cost of financial crime compliance in the U.S. and Canada was upwards of $60 billion in 2023. Forrester Consulting (commissioned by LexisNexis Risk Solutions), True Cost of Financial Crime Compliance Study—U.S. & Canada (2023) (findings deck), https://www.corporatecomplianceinsights.com/wp-content/uploads/2024/02/Forrester-LexisNexis-Risk-Solutions-True-Cost-of-Financial-Crime-Compliance-Study-2023.pdf (last visited Oct. 14, 2025).

must collect and store sensitive identity data to perform many compliance functions, yet need to protect personal information to comply with data protection regulations. Again, these obligations and the related costs and inefficiencies, are several, which compounds the problem. That is why blockchains and oracle networks[3] are such an exciting improvement to customer experience without reducing the necessary standard of compliance.

Blockchains and oracle networks can now support a new and hybrid approach to compliance, particularly through the use of reusable identities that are anchored to blockchain networks. Once identity information is validated and a reference to that identity information is stored onchain by a credible identity provider (e.g., governments or financial institutions), that onchain reference can be reused and verified by other institutions and applications as opposed to repeating the same identity verification process. In practice, this means issuing portable verifiable credentials to individuals and organizations, binding those credentials to strong authenticators, and making them consumable by existing compliance systems within regulated firms. This structure is known as the identity oracle model.

The identity oracle model provides a framework to improve compliance program effectiveness by reducing onboarding pathways that use less reliable means of identity verification. This model also lowers cost by reducing duplicative compliance checks across venues (whether KYC/KYB, AML/CFT, CIP, sanctions screening (e.g., OFAC), accredited investor or other checks) while institutions gain consistent, up-to-date eligibility checks and clearer audit trails. Privacy risk is reduced because proofs stand in for raw personal data, and cybersecurity exposure is narrowed when fewer systems store sensitive data. Additionally, the traceability of public ledgers provides law enforcement and compliance departments with sufficient information to direct requests for underlying information to support investigations and financial intelligence.

Recommendation: For instances in which a customer relationship is established, Treasury should expand current BSA reliance provisions to include all BSA-regulated financial institutions. It should also provide additional guidance to define how financial institutions can satisfy their risk-based customer identification requirements[4] when relying on other financial institutions' and third-party identity providers' collected identity and credentialing information. Under existing FinCEN guidance, a financial institution may only rely on another financial institution to perform its Customer Identification Program ("CIP") procedures when it can show its reliance on such other financial institution was "reasonable" and a contract is signed between the parties, among other requirements.[5] In practice, these requirements prove burdensome and clarity as to the "reasonableness" of whether a financial institution can rely on an onchain credential would help unblock the market. Such guidance should be designed to provide flexibility and describe when financial institutions may rely on information collected by other financial institutions rather than

[3] An oracle is a tool to read offchain data and make that data available to be used onchain, since blockchains do not natively have the ability to consume data from outside their environment. By making information available onchain, oracles allow smart contracts to execute based upon inputs and outputs from the real world. https://chain.link/education/blockchain-oracles

[4] See e.g., 31 CFR § 1020.210 (requiring banks to have "risk-based procedures for conducting ongoing customer due diligence"); 31 CFR § 1020.220 (requiring banks to have a customer identification program that includes "risk-based procedures for verifying the identity of each customer").

[5] FinCEN et al., FAQs: Final CIP Rule 9 (Jan. 2004), https://www.fincen.gov/system/files/guidance/finalciprule.pdf (discussing 31 C.F.R. § 103.121(b)(6) "Reliance").

replicating verification. Additionally, such guidance could set forth standards for credentialing including audit rights and confirming that a particular credential has not been revoked.

In addition, Treasury should engage in a study to explore predicate-based verification (i.e., proving that a credential satisfies a compliance rule without revealing underlying personal data through technologies like zero-knowledge proofs) and work with the industry to understand how such tools can satisfy AML/CFT requirements, sanctions obligations, and FATF Recommendations. We believe that governmental bodies, including law enforcement, should be able to access the underlying information within a reasonable timeframe and certain other requirements are met using this cutting edge technology. In practice this means accepting zero-knowledge or selective-disclosure proofs that confirm, for example, whether a particular customer is approved to trade a specific asset at that time. Whether the proof is verified by an offchain system or by a smart contract prior to settlement, it should count as a compliant check if prescribed conditions are met. This approach lets institutions record exactly what policy was satisfied, by which issuer, at what assurance level and time, without storing documents or raw attributes.

2. Distinguishing administrative control from customer relationships

A wallet calling a function within a smart contract should not create a customer relationship between the administrator of the contract and the owner of the wallet. Similar to traditional finance, there are many instances in which a person's interaction with a financial institution or other third-party does not establish a customer relationship. For example, the endorsement of a check to a third-party does not create a customer relationship between the check holder and the bank that printed it. By making this distinction, Treasury could foster innovation by ensuring software providers are not inadvertently subject to financial regulation.

Recommendation: Treasury should provide guidance distinguishing (i) administrative control of a smart contract published by a software provider, which does not create a customer relationship, from (ii) a person that has possession or control of assets, which creates a customer relationship. Within this guidance, Treasury should reiterate its long-held position that a person can implement policies and procedures to prevent their designation as a BSA-regulated financial institution. Since 2006, Treasury has held to guidance that "a business that develops and implements written policies and procedures that would exclude it from the definition of money services business would cease to be, and would not be treated as, a money services business for the purposes of the Bank Secrecy Act."[6] Treasury has applied this guidance to check cashers that do not cash checks above $1,000 and to sellers of prepaid cards that do not sell more than $10,000 to a single person in a single day. Similarly, Treasury should reiterate that an administrator of a smart contract that *has the ability* to take possession or control of third-party assets is not a money services business so long as it has implemented policies and procedures that exclude it from exercising such ability in the ordinary course of business, with appropriate limitations for exigent circumstances.

[6] FinCEN, FIN-2006-G006 Registration and De-Registration of Money Services Businesses (Feb. 03, 2006).

3. Rules engines allow financial institutions to satisfy their compliance obligations onchain

Another challenge financial institutions face with respect to mitigating illicit activity is how to apply existing compliance infrastructure to onchain transactions. Initial attempts have been expensive, slow, or incomplete, such as relying on manual and duplicative processes, doing point integrations with dozens of different vendors, or using third parties to manage compliant/non-compliant lists of onchain addresses. To address this problem, oracle networks and smart contracts can embed compliance policies directly onchain as rules engines, such as the Chainlink Automated Compliance Engine.[7]

Automated rules engines enable financial institutions and blockchain applications to define and enforce compliance policies, leveraging portable identity credentials and connecting to other established blockchain analytics providers (e.g., Chainalysis, Elliptic, etc.). These institution-directed policies can include pre-transaction eligibility checks (e.g., KYC, AML, CFT, sanctions, etc.), transaction volume rate limits, holds on accounts, and other restrictions required by financial institutions to meet their compliance obligations.

Rules engines are effective because their policies are enforced prior to transaction settlement and on an automated basis so that high-risk transactions do not finalize unless specific compliance policies are satisfied. Because the checks occur prior to settlement, suspicious flows do not occur, and the resulting onchain events form an immutable audit trail that examiners can trace without reconstructing intent after the fact. These controls integrate with offchain analytics that evaluate exposure to mixers, sanctioned entities, or bridge-based obfuscation and provide provenance for decisions.

Recommendation: We propose that Treasury engage in a study to explore how financial institutions can use automated rules engines to satisfy their compliance obligations, with a focus on principles for financial institutions to satisfy their risk-based requirements rather than prescribing specific technology implementations. Automated compliance processes, such as rules engines, are an improvement over existing compliance functions because they help avoid human error-related compliance gaps, and Treasury should study this technology-forward solution to automating compliance and consider encouraging the market around rules engines to mature.

4. Proof of Reserve and Secure Mint highlight the benefits of technology-enforced compliance

The GENIUS Act's monthly disclosure and examination requirements establish a baseline for reserve transparency, but it can and should go further in terms of consumer protection. Cryptographic assurance can extend that baseline by connecting offchain reserve data to onchain systems to create automated reserve attestations, and by encoding secure-mint logic that prevents new issuance when reserves fall short of policy thresholds. In this design, custodial balances or other reserve proofs are attested and made

[7] The Chainlink Automated Compliance Engine (ACE) is a suite of onchain smart contracts and offchain services that are intended to enable financial institutions to programmatically enforce compliance policies when transacting in a blockchain environment. Chainlink ACE is a modular framework comprising of a rules engine (which automatically enforces pre-defined rules onchain), an identity manager (which links real-world identities to onchain credentials without storing PII onchain, and makes those credentials available on any chain), and a monitoring and reporting manager (which provides real-time alerting), among other features.
https://blog.chain.link/automated-compliance-engine/

available to compliance systems and minting contracts; if reserve coverage dips below a pre-defined ratio or a required attestation is stale, minting is automatically disabled until the condition clears, which helps prevent against market depegs and infinite mint hacks. The effect need not replace accounting oversight, but to add continuous, objective checks that are visible to both institutions and supervisors. This transparency sharpens detection of anomalies (for example, sudden drawdowns inconsistent with issued supply) and narrows the window in which misstatements could propagate into markets.

Recommendation: To foster adoption while standards mature, Treasury should clarify that automated reserve attestations and secure-mint gating are acceptable supplemental controls within a comprehensive compliance program, subject to appropriate third-party risk management. Because oracle and attestation networks provide critical inputs, it would also be useful to recognize them explicitly within third-party risk guidance so financial institutions can leverage these utilities with clear regulatory footing.

***

We appreciate Treasury's leadership in seeking practical, technology-forward methods to detect and mitigate illicit finance risks involving digital assets. The recommendations described above—portable digital identity verified through identity oracles, distinguishing administrative control from customer relationships, rules-based onchain compliance, and cryptographically assured reserve transparency—can measurably improve detection and reduce risk while aligning with the GENIUS Act's goals. Chainlink Labs would welcome the opportunity to provide further information to support Treasury's research and any subsequent guidance or rulemaking.

Respectfully submitted,

Chainlink Labs
Benjamin Sherwin
General Counsel