May 15, 2026

Jennifer M. Jones, Deputy Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street NW
Washington
DC 20429

Re:	**Comment on RIN 3064–AG20: Approval Requirements for Issuance of Payment Stablecoins by Subsidiaries of FDIC-Supervised Insured Depository Institutions**
Submitted:	**VIA ELECTRONIC TRANSMISSION to comments@fdic.gov**
Primary Contact:	[redacted]

Dear Ms. Jones:

Chainalysis Inc. (Chainalysis) appreciates the opportunity to comment on the Federal Deposit Insurance Corporation's (FDIC) notice of proposed rulemaking (NPRM).

Background on Chainalysis Inc.

Chainalysis is a blockchain data platform that enables safer, more secure use of public blockchains by banks, businesses, and governments. We provide blockchain analytics, investigative, and risk management technologies used by financial institutions, regulators, and law enforcement agencies to support compliance with anti-money laundering (AML), countering the financing of terrorism (CFT), economic sanctions, and other financial integrity requirements.

Through our work with regulated banks and financial institutions that interact with public blockchain networks, including through custody, payments, and digital-asset issuance, we have developed practical insight into how blockchain analytics intersects with financial integrity and supervisory objectives, while recognizing that multiple approaches can support effective compliance. These tools and data are used to analyze blockchain activity and identify illicit financial flows. To date, we have supported public-sector partners in recovering more than $35 billion in cryptoassets linked to illicit activity worldwide. We also support private-sector institutions in managing their financial crime and sanctions risk.

Foreword

We recognize the FDIC's objectives of prioritizing safety and soundness, supporting responsible innovation, and minimizing unnecessary regulatory burden for applicants seeking approval to become permitted payment stablecoin issuers (PPSIs) under the GENIUS Act. We appreciate the FDIC's effort to establish clear standards and a defined review timeline for PPSI applications.

The effectiveness of the proposed rulemaking will depend in part on whether applicants and supervisors share a common understanding of what effective compliance and risk management look like in practice. While flexibility is important, a lack of supervisory clarity, particularly regarding

on-chain AML, sanctions, and operational risk controls, may result in inconsistent application outcomes, uneven risk mitigation, or unnecessary uncertainty for both applicants and examiners.

Payment stablecoins differ from traditional banking products in ways that are directly relevant to safety and soundness, including the transparency, speed, and global reach of blockchain-based transactions. Compliance frameworks designed for traditional payment systems may therefore require adaptation to remain effective in blockchain environments.

Recent experience in the banking sector also shows that institutions with digitally native business models, significant upfront capitalization, and specialized customer bases may scale activity rapidly following approval. In such cases, the effectiveness of compliance and risk management frameworks depends not only on governance and financial resources, but also on the institution's ability to identify and manage technology-driven risks from inception.

Clearer supervisory expectations, whether through regulatory text, guidance, or examination practice, would help ensure that innovation proceeds alongside consistent compliance standards and does not create supervisory gaps or blind spots.

We note that the FDIC's proposed rulemaking addresses the application process for PPSI subsidiaries of FDIC-supervised institutions, while other primary Federal payment stablecoin regulators are concurrently developing broader substantive frameworks under the GENIUS Act. In preparing this response, we have sought to offer observations that are relevant to the FDIC's specific proposal while recognizing the importance of consistency across supervisory approaches. Many of the themes addressed in this letter, particularly relating to blockchain analytics quality, on-chain risk management, and integrated compliance frameworks, are, in our view, relevant across the supervisory landscape and may benefit from coordinated treatment to avoid regulatory fragmentation. We would welcome the opportunity to engage with the FDIC and other regulators on these cross-cutting issues.

The recommendations in this letter depend on the ability to monitor publicly available on-chain transaction data. Monitoring public ledger data is not a privacy violation. Customer personal information must be protected, but analyzing publicly available blockchain transactions for compliance purposes is a different activity entirely, and must not be restricted.

This letter response addresses five areas:

I. Application format considerations;
II. AML/CFT and sanctions compliance for on-chain activity, including the role of blockchain analytics as both a compliance capability and a supervisory tool, and the quality standards on which effective analytics depend;
III. Integrated upstream and downstream compliance frameworks that connect smart contract security with transaction monitoring;
IV. Consortium governance in multi-institution stablecoin arrangements; and
V. Implementation burden, including practical guidance for applicants, supervisory capabilities, and efficiency considerations.

Responses to Questions

I. Application Format Considerations

Relevant to Question 2

While we defer to the FDIC's judgment on the appropriate format for application, we observe that a structured form, particularly if it is digital and includes defined call and response-type questions, could support more consistent examiner evaluation of on-chain compliance capabilities across applications. This, in turn, may reduce uncertainty for both applicants and examiners in assessing what constitutes an effective compliance framework for blockchain-based activities. As we detail in our response, we believe that an important addition would be questions around on-chain transaction monitoring capabilities, blockchain-specific risk assessment methodologies, and the quality and coverage of analytics tools employed.

II. AML/CFT and sanctions compliance practices with respect to on-chain activity

Relevant to Questions 3, 4, and 7

The proposed rulemaking appropriately requires applicants to submit policies and procedures addressing Bank Secrecy Act (BSA), AML, CFT, and economic sanctions compliance for both on-chain and off-chain transaction processing. These controls are central to the FDIC's assessment of safety and soundness.

Payment stablecoins raise compliance considerations that differ from those associated with traditional payment instruments. Since transactions are recorded on transparent, immutable blockchain ledgers without intermediaries, effective compliance programs require visibility into transaction flows and counterparties beyond what can be derived solely from customer-identity information.

This is significant given the scale and trajectory of stablecoin-related illicit activity. Stablecoins have become the dominant asset class in illicit virtual asset flows, accounting for approximately 63% of illicit transaction volume in 2024 and rising to around 84% in 2025, up from a minority share just a few years ago when Bitcoin dominated illicit flows. [1] This shift reflects the same characteristics that make stablecoins attractive for legitimate payment use (price stability, fast settlement, and cross-chain interoperability) and reinforces the importance of compliance tools specifically designed for stablecoin monitoring, rather than reliance solely on controls developed for traditional payment rails.

i. Blockchain analytics as a compliance capability for PPSI applicants

In practice, many regulated institutions engaged in blockchain-based activities, including PPSIs, supplement customer-based controls with transaction- and address-level risk analysis using blockchain analytics. This can identify exposure to illicit activity typologies such as fraud, ransomware, sanctions evasion, terrorist financing, and the misuse of anonymity-enhancing services, including in cases where exposure does not originate from a known customer.

These capabilities are particularly relevant for institutions serving globally active technology firms, digital-asset businesses, or other clients transacting at scale across jurisdictions. In such environments, risk often first emerges at the address or smart contract level before becoming visible through account- or customer-level controls.

Section 4(a)(5) of the GENIUS Act treats PPSIs as financial institutions for purposes of the BSA and subjects them to all applicable Federal laws relating to economic sanctions, prevention of money laundering, customer identification, and due diligence. In practice, meeting these obligations for stablecoin-native activity requires monitoring capabilities that can operate at the speed and scale of blockchain transactions.

The GENIUS Act also requires PPSIs to maintain the technical capacity to freeze, seize, or burn tokens upon lawful order. In this regard, blockchain analytics is a practical prerequisite for exercising this capability effectively: identifying which addresses or transactions to act upon, quantifying exposure, and maintaining auditable records of the basis for action. Major stablecoin issuers have already demonstrated the operational value of this approach: between 2023 and 2025, Tether alone froze over USD 3.3 billion across more than 7,000 addresses at law enforcement request, cooperating with more than 275 agencies across 59 jurisdictions. [2]

Effective blockchain analytics are what make this targeted, evidence-based enforcement action possible. Here is what this looks like in practice. A sanctioned entity uses a PPSI's stablecoin to move $2 million through a chain of intermediary wallets to a centralized exchange. Blockchain analytics detects the sanctioned address, traces the funds through each intermediary hop, flags the exposure to the PPSI's compliance team, and generates an auditable record supporting a freeze action. This happens all before the funds reach the exchange. Without analytics, the PPSI would have no visibility into this activity: the sanctioned entity is not the PPSI's customer, the intermediary wallets are pseudonymous, and the transactions occur on a public ledger the PPSI has no inherent reason to monitor.

ii. Blockchain analytics as a supervisory tool for FDIC examiners

In the context of FDIC application review, blockchain-native monitoring capabilities can provide examiners with concrete, auditable evidence of how an applicant identifies and manages on-chain risk. Transaction- and address-level analytics generate reviewable outputs, such as exposure analyses, alert histories, and typology-based risk assessments, that can be assessed alongside traditional BSA/AML documentation. This can support more consistent supervisory outcomes and reduce uncertainty in determinations of application completeness.

Effective evaluation of an applicant's on-chain compliance posture may require examiners to have access to independent analytical capabilities, not only to review documentation submitted by the applicant, but to verify the applicant's claims against observable on-chain activity.

The proposed rulemaking appropriately notes that the FDIC would, wherever possible, utilize information already available to it as the primary Federal regulator of the applicant. However, for PPSIs, the relevant "information" includes on-chain transaction activity that is not captured by traditional supervisory or examination information systems. Without independent access to blockchain analytics, examiners may be limited to evaluating an applicant's compliance narrative rather than independently assessing its on-chain exposure profile, the effectiveness of its monitoring systems, or the accuracy of its risk representations. As such, the FDIC may wish to consider equipping its examination function with blockchain analytics capabilities that would allow examiners to independently assess applicants' on-chain compliance posture at the application stage and on an ongoing supervisory basis.

iii. On-chain compliance policies and procedures

With respect to the types of policies, procedures, and customer agreements necessary to evaluate the statutory factors (Question 7), we observe that effective on-chain compliance programs typically go beyond binary sanctions screening, which, while necessary, is insufficient for the full range of risks that stablecoin transactions present. Policies and procedures that the FDIC may wish to consider as relevant to its assessment include those addressing:

- Network-based counterparty exposure analysis, systematically assessing whether an applicant's on-chain counterparties connect to high-risk services, including services that have both direct or indirect connections to illicit activity typologies such as fraud, ransomware, sanctions evasion, or anonymizing infrastructure;

- Behavioral analytics, applying rules and models to flag on-chain transaction patterns inconsistent with expected activity, such as rapid cycling of large amounts, structured transactions, or concentrated interactions with high-risk clusters; and

- Cross-chain monitoring, given that payment stablecoins increasingly operate across multiple blockchain networks (including Ethereum, Tron, Solana, and others), applicants' monitoring capabilities should extend across all chains on which their stablecoins are issued or transacted, rather than being limited to a single network.

Clarifying these expectations in the final rule or accompanying guidance would assist both applicants in preparing thorough filings and examiners in evaluating the adequacy of proposed compliance programs. Specifically, we suggest clarification that;

- PPSI applicants may demonstrate compliance with section 4(a)(5) of the GENIUS Act through the use of blockchain-native monitoring and risk assessment capabilities alongside traditional BSA/AML tools;

- Issuance on public or decentralized blockchain networks, when supported by appropriate monitoring, controls, and governance, is consistent with the statute's safety and soundness objectives; and

- Compliance resources should be allocated, consistent with risk-based principles, to higher-risk activities that blockchain analytics can help identify. A purely performance-based approach, requiring effective monitoring without specifying the technology, is not viable here. No other category of tool can attribute pseudonymous addresses to real-world entities, trace cross-chain fund flows, or screen against sanctions designations at the address level. Specifying blockchain analytics as a required capability is not mandating a vendor; it is recognizing a technology category, in the same way that regulators require credit risk models without prescribing which model a bank must use.

i. Blockchain analytics quality and reliability

In assessing PPSI applications, we would caution against treating the presence of blockchain analytics as a binary tick box exercise. Not all blockchain analytics solutions are equivalent, and a compliance framework that merely confirms an applicant has analytics tooling, without evaluating the quality and methodology of that tooling, risks creating a false sense of assurance. Providers differ meaningfully in the quality, breadth, and methodology that underpins their data, and these differences directly impact compliance and investigative outcomes.

How blockchain analytics works

Blockchain analytics works by grouping raw blockchain addresses that belong to the same entity (structural grouping) and then identifying which real-world person, business, or service controls those addresses (entity attribution) A further analytical step is required to determine whether the identified entity operates the wallet infrastructure or is merely a user or beneficiary of it, a distinction that, if missed, can lead to fundamentally incorrect exposure calculations. The accuracy of these processes determines whether compliance teams and investigators can rely on the results. In our experience, three factors are determinative:

- Attribution rigor: attribution is the process of linking a blockchain address to a known real-world entity, such as an exchange, a sanctions-designated service, or an individual. The reliability of this link depends on how it was established. Attributions grounded in verifiable, empirical evidence, such as confirmed law enforcement data, direct transactional verification, or regulated-entity confirmations, produce materially different outcomes than those based solely on probabilistic inference;

- Structural grouping accuracy: structural grouping is the process of determining which blockchain addresses are controlled by the same entity. On Bitcoin-like blockchains, this can be established with forensic reliability when addresses co-sign the same transaction, proving shared key control. On other blockchains, different techniques are required but the same standard applies: the grouping must be deterministic and reproducible. Errors in clustering are particularly consequential because every attribution, risk score, and compliance decision propagates across the cluster. A single incorrectly included address can contaminate thousands of downstream results; and

- Entity and chain coverage breadth: how many services, wallets, protocols, and blockchain networks are identified and kept current.

Differences across these dimensions between providers are not marginal. Inaccurate clustering can lead compliance teams or investigators to trace funds through the wrong service, generating flawed intelligence. High false positive rates in compliance screening waste resources on irrelevant alerts and erode confidence in the monitoring framework. Incomplete chain or entity coverage creates blind spots that illicit actors can exploit, particularly significant for PPSIs whose stablecoins may operate across multiple blockchain networks simultaneously.

Deterministic and probabilistic outputs

It is also important to distinguish between deterministic and probabilistic analytical outputs of this process, as each serves different compliance functions and carries different evidentiary weight so has direct implications for how they should be considered and used. Deterministic outputs, such as forensically established address clustering, produce conclusions that are reproducible and court-admissible: given the same on-chain evidence and methodology, an independent expert will reach the same result. These outputs form the structural foundation for fund tracing, sanctions enforcement, and freeze or blacklist actions where the evidentiary standard is highest. Probabilistic outputs, such as risk scores derived from machine learning models or behavioral pattern detection, serve a different but complementary function: they enable compliance teams to triage large volumes of transaction activity, prioritize investigative attention, and detect emerging typologies that would be impractical to identify manually. Both are valuable, but the distinction matters for supervisory purposes. Compliance decisions that carry legal consequences, such as suspicious activity reports, freeze actions, or law enforcement referrals, should be grounded in deterministic evidence. Compliance functions that involve risk prioritization, alert generation, and pattern detection benefit from probabilistic signals. A high-quality blockchain analytics solution should offer both, never conflate them, and be transparent about which outputs rest on which evidentiary basis.

Quality standards and independent verification
These are not theoretical concerns. They have been tested in both judicial and academic settings:

- In United States v. Sterlingov (Bitcoin Fog, 2024), a US federal court applied Daubert standards to assess the reliability of blockchain analytics evidence and ruled that the methodology met the threshold for admissible expert testimony, finding it to be "the product of reliable principles and methods." [3]

- In 2025, independent academic researchers from TU Delft published the first peer-reviewed evaluation of a blockchain analytics vendor at the 34th USENIX Security Symposium, one of the world's leading computer security conferences. The study evaluated clustering accuracy against a controlled dataset derived from seized servers and found true positive rates of up to 94.85% with false positive rates below 0.15%. [4]

In the context of the proposed application process, we suggest that the FDIC consider requiring applicants to address analytics quality as part of their filing, rather than treating the deployment of blockchain analytics as sufficient in itself. Specifically, the application could request information on:

- **Minimum benchmarks for blockchain analytics solutions used in PPSI compliance contexts:** Covering attribution methodology, clustering accuracy, entity coverage, chain coverage, and the frequency of data updates. Such benchmarks would assist both applicants in selecting appropriate tools and examiners in evaluating the adequacy of proposed compliance programs.

- **Independent verification:** Encouraging or expecting PPSIs to demonstrate that the analytics providers they rely on have been subject to independent scrutiny, whether through academic peer review, court-tested evidence standards, or supervisory audit. Providers whose methodologies and data quality have been subjected to independent evaluation, whether through academic peer review, court-tested evidence standards, or supervisory audit, offer a materially different level of assurance to regulators than those that have not

- **Methodological transparency:** Expecting PPSI applicants to describe, or make available for supervisory review, the methodology by which their blockchain analytics provider constructs its core analytical outputs. The reliability of compliance decisions depends not only on headline metrics such as entity or chain coverage counts, but on how the provider decomposes the analytical process, including how addresses are structurally grouped into wallets, how those wallets are attributed to real-world entities, and how the provider distinguishes between the operator of a service and a mere user or beneficiary. Where the methodology underlying these determinations is opaque, does not meet a baseline level of expectation, or contractually shielded from independent evaluation, the value of the solution should be considered diminished.

Establishing these expectations at the application stage would support the FDIC's broader objective of ensuring that approved PPSIs can maintain effective compliance programs on an ongoing basis, not just at the point of initial application, and would contribute to a shared understanding between applicants and examiners of what effective on-chain compliance looks like in practice.

III. Recognizing on-chain operational risks as a safety and soundness consideration and requiring an integrated compliance program for comprehensive PPSI risk management

Relevant to Questions 4 and 11

i. The case for a connected security and compliance fabric

In assessing whether an applicant's risk management framework is adequate, the FDIC should consider whether the applicant has addressed threats at all stages of development and deployment, particularly where there is an on-chain footprint, e.g., a PPSI with a smart contract that manages the issuance of its payment stablecoins. In such a scenario, a siloed approach - where security teams focus on upstream operational and technical safeguards while compliance teams design and implement downstream procedures such as transaction monitoring and reporting - creates potentially dangerous gaps in protection and oversight. For example, such blind spots might manifest where:

- PPSI Security teams identify smart contract vulnerabilities without connecting them to their compliance implications, and in doing so, the compliance team would fail to meet an obligation to report any meaningful interruptions or issues with service delivery within a set time period to their regulator or client base (such as the requirements might be structured); or

- PPSI Compliance teams undertaking an organizational risk assessment fail to capture how technical vulnerabilities can manifest as compliance failures and do not consider appropriate response mechanisms. A smart contract exploit that enables unauthorized minting or transfer of stablecoins may simultaneously constitute an operational failure, a potential BSA reporting obligation, and a threat to reserve adequacy, yet a siloed compliance team may not recognize the event as triggering all three consequences without integration with the security function.

Recent academic analysis supports the view that these risks must be addressed as a unified supervisory concern. Researchers at the MIT Digital Currency Initiative, examining the implementation of the GENIUS Act, concluded that "technological risks, arising from smart contract logic, blockchain consensus mechanisms, bridges, oracles, and governance design... may impair transferability or redemption in some circumstances, potentially affecting confidence, even when reserves remain intact." [9] This supports the notion that the FDIC's evaluation of safety and soundness under section 5(c)(1) should encompass operational dependencies on blockchain infrastructure, not solely reserve quality, and that the security and compliance dimensions of those dependencies must be assessed together.

This underscores that technical vulnerabilities and compliance failures are two sides of the same risk coin for PPSIs, and both should be treated equally in application requirements. What is required is an approach that more fully supports the safety and soundness of PPSIs and manages the unique risks of blockchain-based financial products by acknowledging the full range of associated threats and complexities. Both upstream and downstream approaches would combine and complement one another to create a continuous security and compliance fabric that addresses operational and financial crime risks, ensuring the security of their payment stablecoins on both an initial and ongoing basis. When integration of these two is achieved rather than siloed, PPSIs can benefit from:

- Fuller visibility of risks: Technical vulnerabilities and compliance risks are viewed together, revealing how they interrelate

- Faster response times: Security alerts from smart contract monitoring can immediately inform compliance decisions

- More efficient resource allocation: Resources can be directed to the most pressing risks, regardless of which domain they originate from (reducing the risk of duplication of effort)

- Better regulatory preparedness: PPSIs can demonstrate to regulators that they understand and manage the full spectrum of risks unique to blockchain environments and are future-proofed for potential changes

We propose that PPSI applications should evidence a connected security and compliance fabric in which upstream (smart contract, code, etc.) security and operational competency are integrated with downstream (transaction monitoring, etc.) compliance programs. For example, a program that covers code deployment through to transaction monitoring will be essential to establishing a reasonable expectation of safe, sound, and compliant PPSI operations.

1. The Upstream: Requiring PPSI applicants to provide evidence of the use of smart contract security solutions

A comprehensive risk management framework for PPSIs must address vulnerabilities at the foundational smart contract level before considering downstream transaction monitoring. Smart contracts are the foundational layer of stablecoin operations, governing issuance, redemption, transfers, and reserve management. As such, the importance of security tools and associated capabilities to proactively identify vulnerabilities and unusual behavior at the code and protocol level (thereby preventing potential exploits before they can cause harm) represents a critical "upstream protection".

The immutable nature of blockchain means that vulnerabilities in smart contract code, once deployed, can lead to significant financial losses with limited remediation options. For PPSIs, whose stablecoins will likely operate across multiple blockchain networks, ensuring the security of underlying smart contracts is fundamental to operational resilience and soundness. The scale of this risk is significant: over $3.4 billion was stolen through crypto hacks and exploits in 2025 alone, and fewer than 2% of affected projects were able to respond to attacks within the first hour. [6]

Critically, static point-in-time security measures, while necessary, are not sufficient on their own. Industry data indicates that effectively all major smart contract exploits in 2024 and 2025 occurred on projects that had undergone pre-deployment security audits. [7] This underscores that security does not end at deployment: vulnerabilities may be introduced through upgrades, governance changes, or novel attack vectors that post-date an initial audit. International regulators have begun to recognize the importance of security assurance for smart contracts in financial markets. A 2025 joint working group of the French prudential authority (ACPR) and financial markets authority (AMF) examined the need for smart contract certification and auditing standards, reflecting growing supervisory attention to the risks that smart contract vulnerabilities pose to financial stability. However, the working group's focus on point-in-time certification highlights the limitations of static approaches, a gap also recognized in the EU's Digital Operational Resilience Act (DORA), which requires financial entities to maintain ongoing ICT risk monitoring and incident response capabilities rather than relying solely on periodic assessments. [8] We believe these developments reinforce the case for ongoing, real-time monitoring as the baseline for smart contract security in the FDIC's supervisory framework for PPSIs.

For payment stablecoins specifically, smart contract security tools should be capable of identifying threats to supply integrity (such as unauthorized minting or burning of tokens), unauthorized governance or administrative changes (including ownership transfers, proxy upgrades, or modifications to freeze and blacklist functions), reserve management anomalies, and depeg events that may signal underlying technical or operational failures. These categories of risk are directly relevant to the statutory requirements of the GENIUS Act, including the obligation to maintain the technical capacity to freeze, seize, or burn tokens when lawfully ordered. Security tools that monitor

the integrity of these functions provide assurance that the mechanisms themselves have not been compromised or manipulated.

The value of continuous monitoring is further demonstrated by its capacity to support automated defensive responses. Real-time smart contract monitoring tools can be configured to trigger immediate protective actions, such as pausing contracts or initiating asset transfers to secure wallets, when anomalous behavior is detected. The capacity for rapid, automated response is particularly important for PPSIs, where delays in responding to a smart contract exploit could simultaneously threaten reserve adequacy, disrupt redemption operations, and trigger regulatory reporting obligations.

We respectfully suggest that the FDIC explicitly recognize smart contract security assessment as a core component of PPSI compliance frameworks, requiring applicants to demonstrate:

- Rigorous pre-deployment security audits of all smart contracts governing stablecoin issuance, redemption, and reserve management;
- Continuous, real-time monitoring of smart contract interactions for anomalous behavior that could indicate exploits, technical vulnerabilities, or unauthorized changes to contract governance, including supply integrity, access controls, and reserve management functions;
- Defined automated response capabilities that enable rapid defensive action when smart contract anomalies are detected, consistent with the institution's incident response and business continuity frameworks;
- Implementation of security best practices, including formal verification where appropriate; and
- Integration of smart contract security outputs into downstream compliance workflows, ensuring that upstream security events inform transaction monitoring, suspicious activity reporting, and regulatory notifications as part of the connected security and compliance fabric described above.

2. The Downstream - Requiring PPSI applicants to provide evidence of the use of blockchain analytics as part of entity and transaction-level compliance programs

With upstream smart contract security addressed, the downstream compliance layer (detailed in Section II) concerns how PPSIs monitor and manage risk at the transaction and entity level. Two scenarios illustrate why this capability is essential to operational resilience:

- Exposure to illicit finance or sanctioned actors through on-chain interactions, with potential legal, reputational, and operational consequences.
- Adverse on-chain events such as sanctions designations, law enforcement actions, or major blockchain incidents that require a rapid assessment of historical and ongoing exposure to specific addresses or services.

In each case, blockchain analytics enables the rapid response that traditional compliance tools cannot: timely lookbacks across an institution's full on-chain history, real-time exposure quantification, and ongoing monitoring following designations or enforcement actions. These capabilities are particularly important during periods of market stress, when institutions must act quickly to preserve orderly redemption and stable operations.

We therefore encourage the FDIC to explicitly recognize on-chain illicit finance and sanctions exposure as operational risks relevant to PPSIs, both at the application stage and in ongoing supervision. As discussed further in Section V, meaningful assessment of an applicant's on-chain risk posture is most effective when examiners themselves have access to blockchain analytics tools for independent verification.

ii. Governance integration

From a governance perspective, effective use of blockchain analytics depends on clear ownership and escalation within an institution's compliance and risk management framework. PPSIs may be better positioned to demonstrate safety and soundness when on-chain risk identification informs defined decision-making processes, including sanctions reporting, suspicious activity reporting, and oversight by senior management or the risk committee. Clarifying how on-chain findings are reviewed, escalated, and acted upon may help supervisors assess whether analytics capabilities are meaningfully integrated into the institution's broader control environment.

IV. Multi-institution stablecoin arrangements

Relevant to Question 6

The proposed rulemaking appropriately addresses scenarios in which payment stablecoins may be issued through consortium or multi-bank arrangements. While these structures may offer efficiencies, they can also introduce additional complexity in governance, compliance responsibilities, and risk management.

In consortium models, unclear allocation of responsibility for on-chain monitoring, sanctions response, or regulatory engagement can increase operational and supervisory risk. Clear assignment of responsibilities and consistent standards across participants are therefore important both at the application stage and during ongoing supervision. For example, a lead institution might be designated to oversee transaction monitoring across the consortium, with clear reporting obligations to all member institutions.

Consortium arrangements also present specific challenges for the consistency and quality of on-chain compliance. Where different consortium members deploy different blockchain analytics providers, or analytics solutions of varying quality, coverage, or methodology, the result may be inconsistent risk identification across the arrangement. One member institution may flag a counterparty as high-risk while another, relying on a different provider with narrower entity coverage or less rigorous attribution methodology, may not. This inconsistency can create both compliance gaps and supervisory uncertainty.

We suggest the FDIC consider whether additional guidance would be helpful to clarify:

- How responsibility for on-chain transaction monitoring and compliance should be allocated among consortium participants; and
- How shared or coordinated monitoring and reporting approaches may support consistent risk identification and supervisory transparency.

V. Application burden and implementation considerations

Relevant to Question 10

We appreciate the FDIC's efforts to estimate application burden and limit unnecessary regulatory costs. At the same time, designing and implementing effective compliance frameworks for payment stablecoins, particularly those involving public blockchain networks, often requires specialized expertise and operational planning beyond initial application materials. In our experience, much of the uncertainty and potential inefficiency in this process stems not from the volume of requirements themselves, but from a lack of clarity about what constitutes effective implementation in practice.

To that end, we offer observations across three areas of implementation that we believe could help reduce burden for both applicants and examiners, or at least inform potential considerations of cost and complexity by establishing shared expectations:

- Firstly, we suggest practical implementation guidance, including phased deployment timelines and staff training standards, that would help applicants build robust capabilities without unnecessary cost or delay.

- Secondly, we consider the supervisory and examination capabilities that the FDIC itself may wish to develop, as effective oversight of PPSIs will require examiners to engage directly with on-chain data.

- Third and finally, we note the efficiency and cost benefits that blockchain analytics can deliver, which may offset the upfront investment required and reduce the ongoing operational burden of PPSI compliance.

ii. Implementation guidance for applicants

With the analytics quality framework established in Section II, we encourage the FDIC to consider providing practical guidance to assist PPSI applicants in building effective on-chain compliance capabilities. In particular, we suggest:

- Recognizing blockchain analytics as a core capability for PPSI applicants and issuing guidance to assist firms. This might include best practices for implementing compliance tools, performance metrics to evaluate the effectiveness of specific analytics solutions (e.g., minimum quality standards, including coverage completeness and accuracy), and integration protocols with existing compliance systems.

- Engaging with applicants on technical implementation timelines that reflect the complexity of building robust on-chain monitoring and surveillance capabilities and systems, and consider phased approaches that allow for alert calibration (to establish appropriate thresholds for a business) and compliance monitoring, testing, and refinement (e.g., managing false positive/negative rates) to ensure effective integration before full production deployment.

- Establishing expectations for PPSI compliance personnel to develop technical proficiency beyond traditional financial-compliance training. PPSIs should implement ongoing training protocols covering the practical application of blockchain analytics platforms, interpretation of on-chain data patterns, recognition of emerging typologies, and integration of analytics findings into compliance workflows. The FDIC should consider establishing baseline competency standards for blockchain analytics proficiency among PPSI compliance staff, similar to existing professional certification requirements in traditional compliance domains.

iii. Supervisory and examination capabilities

The FDIC should also consider the expertise and resources supervisors and examiners will need to effectively oversee PPSIs and their compliance programs. Public blockchain data offers an opportunity to develop a structurally different mode of supervision for PPSIs, one that goes beyond

traditional sample-based examinations to enable full-population, real-time analysis of on-chain activity. [5] As discussed in Section II, effective supervision requires examiners to engage with on-chain data directly, not merely to review compliance documentation. This capability is important both at the application stage, where examiners must determine whether proposed compliance frameworks are adequate, and in ongoing supervision, where examinations of PPSIs will need to include assessment of on-chain compliance effectiveness.

In practice, blockchain analytics could support the FDIC's supervisory function across the full lifecycle of PPSI oversight:

- At the application stage, examiners could assess the on-chain footprint of an applicant's existing or proposed stablecoin activity and its primary counterparties, gaining independent insight into the applicant's actual risk exposure and comparing it against the applicant's declared risk appetite and proposed compliance framework.

- On an ongoing basis, examiners could track on-chain metrics directly relevant to safety and soundness, such as: total circulating supply of the stablecoin across all chains (which can be compared against records of the value of reserves); the degree of exposure of the stablecoin's market makers and distributors to illicit activity or higher-risk services; the distribution of the stablecoin across exchanges, DeFi protocols, bridge contracts, and personal wallets; and, where available, signals of geographic distribution that can be cross-checked against the issuer's declared customer base and risk mitigation strategies.

- On a market-wide basis, monitoring dashboards can provide a top-down view of the PPSI population, enabling identification of institutions or counterparties with exposure to sanctioned entities, mixing services, or other high-risk infrastructure, supporting risk-based prioritization of supervisory attention across the FDIC's portfolio of PPSI-supervised institutions.

In particular, the FDIC may wish to consider:

- Equipping FDIC examination teams with blockchain analytics tools that enable independent assessment of PPSI on-chain activity, exposure, and compliance effectiveness;

- Developing blockchain-specific examination procedures, whether through updates to the FFIEC BSA/AML Examination Manual or through FDIC-specific guidance, that provide examiners with a structured methodology for evaluating on-chain compliance programs, including criteria for assessing the quality of the analytics tools employed by PPSIs; and
- Investing in ongoing training for examination staff to build and maintain proficiency in blockchain analytics interpretation, on-chain typology recognition, and the evaluation of blockchain-native compliance frameworks.

These investments would support the FDIC's ability to exercise effective oversight of a novel and rapidly evolving class of supervised entity, and would complement, rather than duplicate, the compliance capabilities that PPSIs are themselves expected to maintain.

iv. Efficiency and cost considerations

Blockchain analytics can deliver meaningful efficiency gains that offset the implementation costs described above. Industry wide, compliance teams using blockchain analytics can screen transactions against verified attribution data rather than broad risk indicators, reducing the volume of alerts requiring manual investigation. Institutions deploying automated transaction monitoring have reported reducing investigation cycle times from hours to minutes for routine alert disposition, and real-time on-chain monitoring eliminates the need for costly retrospective lookback exercises by

maintaining continuous compliance coverage. For supervisors, the ability to examine full-population on-chain data rather than relying on sample-based reviews can substantially reduce the cost and duration of examination cycles while improving their thoroughness. The FDIC should recognize these efficiency considerations when evaluating the operational burden of PPSI applications. However, while implementing blockchain-specific monitoring requires an initial investment, the reduction in ongoing compliance costs, faster response to emerging risks, and more efficient supervisory engagement represent a net reduction in operational burden over the lifecycle of a PPSI.

Conclusion

The proposed rulemaking provides a strong foundation for integrating payment stablecoins into the regulated banking system while protecting financial integrity and supporting innovation. Clarifying supervisory expectations for on-chain monitoring, blockchain-specific operational risk, consortium governance, and the quality and reliability of the analytics tools on which compliance programs depend would further strengthen this framework and support consistent outcomes for applicants and examiners alike.

As the FDIC and other primary Federal payment stablecoin regulators advance their respective implementations of the GENIUS Act, we believe that coordinated expectations regarding blockchain analytics quality, integrated compliance frameworks, and examiner proficiency would benefit the supervisory community as a whole. We look forward to engaging with the FDIC on these issues in this and related proceedings, and would welcome continued engagement as a technical resource on blockchain-related compliance, financial crime risk, and operational considerations.

Respectfully submitted,

Chainalysis Inc.

Notes

[1] Chainalysis, 2025 Crypto Crime Report (January 2025); Chainalysis, 2026 Crypto Crime Report (January 2026).

[2] Based on publicly available on-chain data and Tether public disclosures regarding freeze and blacklist actions (2023–2025).

[3] *United States v. Sterlingov* (Bitcoin Fog), Daubert Order, US District Court, District of Columbia, 2024.

[4] Lubbertsen et al., "Evaluating Commercial Blockchain Intelligence," 34th USENIX Security Symposium, 2025.

[5] Chainalysis developed this argument in detail in our October 2025 response to the Department of the Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets (90 Fed. Reg. 40148), in which we outlined how blockchain analytics can support supervisory workflows at the policymaking, application, and ongoing supervision stages for stablecoin issuers.

[6] See note 1, supra; see also industry analysis of smart contract exploit response times across major blockchain networks, 2024-2025.

[7] See, e.g., industry reporting on the state of web3 security (2025), noting that effectively all major smart contract exploits in 2024-2025 occurred on projects that had undergone prior security audits.

[8] See ACPR-AMF Joint Working Group findings on smart contract certification and auditing (2025); see also Regulation (EU) 2022/2554 (Digital Operational Resilience Act), Articles 9-13.

[9] Aronoff et al., The Hidden Plumbing of Stablecoins: Financial and Technological Risks in the GENIUS Act Era, MIT Digital Currency Initiative (February 2026)