

MOHAMMAD NASIR UDDIN

Proposal and Comment Information

Title: Implementing the Federal Reserve Board's Responsibilities under the GENIUS Act, R-1899

Comment ID: FR-2026-0033-01-C19

Subject

Docket No. R-1899; RIN 7100-AH29 — Comment on Proposed § 247.13 (GENIUS Act)

Submitter Information

Name: Mohammad Nasir Uddin

Submitted Date: 10/10/2026

NONCONFIDENTIAL // EXTERNAL

Dear Secretary McDonough,

Please find attached my comment letter on the Board's notice of proposed rulemaking, "Implementing the Federal Reserve Board's Responsibilities Under the GENIUS Act" (Docket No. R-1899; RIN 7100-AH29; 91 FR 61580, September 29, 2026). My comments address proposed § 247.13 and respond to Questions 110, 124, 125, 126, 129, and 132.

Thank you for the opportunity to comment.

Respectfully,

Mohammad Nasir Uddin
Doctoral Student, DBA in Business Intelligence and Data Analytics, Westcliff University
Los Angeles, California
m.uddin.258@westcliff.edu<<mailto:m.uddin.258@westcliff.edu>>

Attachment: GENIUS_Act_Comment_R-1899_Uddin.pdf

October 11, 2026

Benjamin W. McDonough, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

**Re: Implementing the Federal Reserve Board’s Responsibilities Under the GENIUS Act;
Docket No. R-1899; RIN 7100-AH29 (91 FR 61580, September 29, 2026) — Comments on
proposed § 247.13 (Questions 110, 124, 125, 126, 129, and 132)**

Dear Mr. McDonough:

I appreciate the opportunity to comment on the Board’s proposal to implement the GENIUS Act for Board-supervised permitted payment stablecoin issuers (PPSIs). I am an independent researcher and a doctoral student in Business Intelligence and Data Analytics at Westcliff University. My research concerns the governance, validation, and explainability of artificial-intelligence (AI) models used for fraud detection and anti-money-laundering (AML) compliance in U.S. financial institutions. I submit these comments in my individual capacity; my university affiliation is provided for identification only, and I have no financial interest in any stablecoin issuer, blockchain analytics provider, or other party affected by this rulemaking.

My comments are confined to proposed § 247.13 and focus on one issue: the automated and AI-based analytical systems on which Board-supervised PPSIs will depend to meet their risk management and Bank Secrecy Act/AML and sanctions obligations. I support the Board’s principles-based approach and its decision, in proposed § 247.13(d), not to duplicate FinCEN’s and OFAC’s substantive requirements. The suggestions below are intended to be consistent with both choices and to add little burden.

1. The reliability of automated compliance systems is a material risk for PPSIs (Questions 124 and 126)

The proposal recognizes that payment stablecoins can be transferred instantly on a 24/7 basis, that illicit actors can move stolen stablecoins quickly across decentralized exchanges, as in the 2022 Ronin Network hack the Board cites, and that AI tools may increase the risk of future attacks. In that environment, a PPSI’s ability to identify suspicious activity, screen for sanctioned parties, and respond in time will depend heavily on automated analytics: transaction-monitoring systems, sanctions-screening tools, blockchain analytics, and fraud-detection models, increasingly built with machine learning.

These systems can fail in two directions. If they miss illicit flows, the PPSI faces BSA/AML and sanctions exposure and the integrity of the payment stablecoin is undermined. If they generate unreliable alerts, they can cause unwarranted holds or restrictions on legitimate customers. Proposed § 247.13(b)(3)(iii) already requires “evaluation, validation, and reporting processes to ensure that key information technology systems and controls, including smart contracts, are

operating as intended.” I respectfully suggest that the Board make explicit, in the rule text or the preamble, that this validation expectation extends to the models and automated decision systems used for core compliance functions, including transaction monitoring, sanctions screening, blockchain analytics, and fraud detection.

In April 2026, the Board, the OCC, and the FDIC issued revised interagency guidance on model risk management (SR 26-2), which applies to traditional quantitative models and to non-generative, non-agentic AI. A short statement that a Board-supervised PPSI’s governance of material compliance models should be consistent with that guidance, proportionate to the models’ materiality, would give PPSIs clarity without new prescriptive requirements. Where a PPSI uses generative or agentic AI tools, which that guidance excludes from its scope, the Board could indicate that such tools are expected to be governed under the PPSI’s broader risk management framework under § 247.13.

2. Third-party blockchain monitoring providers (Question 125)

The preamble correctly identifies “blockchain monitoring to support compliance with Bank Secrecy Act/anti-money laundering and sanctions requirements” as a function that PPSIs may obtain from third parties. Under proposed § 247.13(a)(5), a PPSI must exercise due diligence in selecting service providers and monitor them “including by reviewing audits, summaries of test results, or other equivalent evaluations.”

For analytical service providers, the most informative “test results” are evidence that the provider’s detection models perform as represented on data resembling the PPSI’s own activity. My research on machine-learning fraud detection has documented several ways in which reported performance can be overstated when evaluation is not strictly separated in time from model development, a problem commonly called data leakage. Leakage occurs, for example, when features, data-scaling parameters, graph connections, or explanation baselines are computed using information from the period or records later used for testing. A model evaluated this way can appear highly accurate in validation and then underperform in production.

I therefore suggest that the preamble indicate that, for material analytical providers, appropriate due diligence and monitoring may include obtaining (i) evidence of out-of-time, independently performed performance testing; (ii) documentation that training and test data were separated so that test results reflect information available at the time of detection; (iii) information on alert explainability sufficient to support the PPSI’s investigations and any suspicious activity reports; and (iv) periodic evidence of ongoing performance monitoring. Where providers treat their models as proprietary, summaries or independent attestations of such testing could satisfy this expectation, consistent with the flexibility already contemplated in § 247.13(a)(5).

3. Network-level and cross-chain risk (Questions 129 and 132)

Illicit activity involving payment stablecoins is typically a network phenomenon: funds move through chains of addresses, intermediaries, and, increasingly, across blockchains, as the Board’s

discussion of the Ronin incident illustrates. Monitoring that evaluates each transfer in isolation can miss these patterns. My published research on explainable graph neural networks for fraud-contagion detection in U.S. interbank payment networks, which is aligned with FinCEN suspicious activity reporting requirements, proposes modeling the relationships among accounts and institutions, together with explanations that tie each alert to the evidence behind it, to support both detection and the preparation of suspicious activity report narratives.

Consistent with the Board's decision not to add AML/CFT requirements beyond FinCEN's, I do not recommend new rule text on this point. Instead, I suggest that the Board consider addressing network-level and cross-chain monitoring in examination procedures or supervisory guidance developed in coordination with FinCEN. Such guidance could note that a PPSI's risk assessment should consider exposure arising from the networks and blockchains on which its payment stablecoins circulate, and that monitoring approaches should be capable of identifying rapid, multi-hop movement of funds associated with hacks, fraud, or sanctions evasion.

4. Keeping the standards principles-based while providing clarity (Question 110)

The Board asks how to keep § 247.13 principles-based while providing sufficient clarity. For automated compliance systems, a brief set of principles could provide clarity without prescribing methods:

- (1) **Proportionality:** validation depth should scale with the materiality of the model to the PPSI's compliance obligations and risk profile.
- (2) **Realistic testing:** performance should be assessed on data separated in time from model development, reflecting conditions the model will face in production.
- (3) **Independence:** validation should be performed by persons, internal or external, who are independent of model development.
- (4) **Ongoing monitoring:** performance should be monitored after deployment for deterioration as transaction patterns and illicit typologies change.
- (5) **Explainability and human review:** alerts that may lead to suspicious activity reports, or to holds or restrictions on customers, should be accompanied by information sufficient for a qualified person to review the basis for the alert.

These principles mirror existing supervisory expectations for banking organizations and can be applied by small and large PPSIs alike.

Conclusion

Payment stablecoins will depend on automated systems to detect illicit activity at the speed at which value can move on distributed ledgers. A modest clarification that these systems fall within the validation expectations of proposed § 247.13, together with supervisory attention to third-party analytics and network-level risk, would strengthen the safety and integrity of Board-supervised

PPSIs and of the U.S. payment system while preserving the proposal's principles-based design. Thank you for considering these comments.

Respectfully submitted,

Mohammad Nasir Uddin

Doctoral Student, DBA in Business Intelligence and Data Analytics, Westcliff University

(affiliation for identification only)

Los Angeles, California

m.uddin.258@westcliff.edu | ORCID: 0009-0009-0990-4616

Relevant research by the commenter

- Uddin, M. N. (2026). A Regulatory Governance Framework for AI-Driven Financial Fraud Detection in US Banking Integrating OCC, SR 11-7, CFPB and FinCEN Compliance Requirements for Model Development, Validation and Monitoring Lifecycles. *Cogent Business & Management* (Taylor & Francis), Article 2724203. <https://doi.org/10.1080/23311975.2026.2724203>
- Uddin, M. N., Anik, A., Orpita, R. T., Bhuiyan, E. R., Risalat, M., & Wali Ullah, S. M. (2026). Explainable Graph Neural Networks for Fraud Contagion Detection and Automated SAR Generation in U.S. Interbank Payment Networks: A FinCEN-Aligned Framework. *Proceedings of the 2026 IEEE AIMS Conference*. <https://doi.org/10.1109/AIMS71270.2026.11712793>
- Uddin, M. N. (2026). Governing AI in U.S. Banking: A Practical Compliance Roadmap for Financial Fraud Detection Systems Under OCC, SR 11-7, CFPB, and FinCEN Requirements. *Banking & Financial Services Policy Report* (Wolters Kluwer), 45(7).
- Uddin, M. N. When Does Shapley-Guided Ensembling Help? A Leakage-Controlled Chronological Evaluation of SGAE for Explainable Financial Fraud Detection. Manuscript under review, *CAAI Transactions on Intelligence Technology*. Code and leakage audit: <https://github.com/nasiruddinstudents-ctrl/SGAE-XAI-Fraud-Detection>