BURAK OKTENLI

Proposal and Comment Information

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

Comment ID: FR-2026-0033-01-C39

Submitter Information

Name: Burak Oktenli

Submitted Date: 11/18/2026

November 18, 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 Fed. Reg. 61580, September 29, 2026)
Dear Mr. McDonough:
I appreciate the opportunity to comment on the Board's proposal to implement the GENIUS Act (Pub. L. 119-27). I am an independent researcher in Washington, DC, and my work concerns how authority is governed and verified when automated and AI-enabled systems act on behalf of people and institutions. I submit this comment in my individual capacity and have no financial relationship with any payment stablecoin issuer, custodian or digital asset service provider.
My comment addresses one question that the proposal's risk-management and custody standards do not yet answer directly: when software acting for a customer initiates a payment stablecoin transfer or redemption, what shows that the instruction was within the authority the customer gave? It responds to Questions 106, 110, 117, 124, 126, 128, 163, 181, 187, 193, 239, 246, 249 and 251.
1. A valid transfer is not necessarily an authorized one
A transfer can be backed by compliant reserves, signed with a valid key and recorded correctly on a distributed ledger, and still be one the customer never intended. Consider a business that uses an automated agent to pay an overseas supplier in payment stablecoins. A forged invoice changes the supplier's address. The agent reads the invoice and initiates the transfer, and a signing service approves it under credentials the business granted. The ledger now records a technically valid transfer. What is missing is evidence that the business approved the new beneficiary. No reserve report, however accurate, answers that question.
This is not a risk that only artificial intelligence creates; ordinary credential compromise and weak payment controls can produce the same loss. What changes with automated agents is the speed and reach of software that turns instructions into payments, and its exposure to manipulated inputs. NIST's taxonomy of adversarial machine learning (NIST AI 100-2 E2025, March 2025) describes indirect prompt injection, in which content that an AI system processes, such as a document or web page, carries instructions that change what the system does. An invoice is exactly such content.
The preamble notes that artificial intelligence tools may be used to find and exploit weaknesses in online portals and smart contracts (91 Fed. Reg. at 61610, 61623). A distinct risk arises when automated tools act through valid interfaces on a customer's behalf. The information technology and security standards in proposed § 247.13(b) address private key management, whether smart contracts operate as intended, and the protection of customer records against unauthorized access. These controls are necessary: they secure the means of signing and recording a transaction. They do not by themselves establish that a given instruction fell within the customer's grant of authority, which is the evidence a customer, an issuer or custodian, and a supervisor will each need when a delegated transaction is disputed.
2. Recommendations
(a) Treat delegated and automated instructions as a named risk area (Questions 110, 124 and 126). Where a Board-supervised permitted payment stablecoin issuer (PPSI) or a Board-supervised custodian executes transfers or redemptions on instructions from automated systems acting for customers, its risk and control framework under proposed § 247.13 should address how it establishes that each instruction falls within the authority the customer granted. This applies equally to a PPSI that holds digital assets on a customer's behalf (see 91 Fed. Reg. at 61611 n.62). A principles-based standard would suffice; the Board need not prescribe a specific technology.
(b) Preserve a record of the payment mandate for consequential delegated transactions (Questions 126 and 128). The record should connect the transfer or redemption to the permission in force when it was

initiated: the authorized payer; the intended beneficiary or controlled list of beneficiaries; the asset and network; the maximum amount or exposure; the validity period; and the party responsible for approving exceptions. A change to the beneficiary or to a spending limit should require fresh authorization under the applicable rules. An automated system's explanation of an instruction, or its stated confidence, should not itself expand the mandate. The record should be available to the customer, and to supervisors and investigators as appropriate. To protect customer privacy, it need not be published on a public ledger, and it can be retained off-chain under the record-protection and retention standards in proposed §§ 247.13(b)(5) and 247.14(g).

(c) Clarify custodians' evidence of customer direction (Questions 181, 187 and 193

Submitted via federalreserve.gov/apps/proposals

November 18, 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 Fed. Reg. 61580, September 29, 2026)

Dear Mr. McDonough:

I appreciate the opportunity to comment on the Board's proposal to implement the GENIUS Act (Pub. L. 119-27). I am an independent researcher in Washington, DC, and my work concerns how authority is governed and verified when automated and AI-enabled systems act on behalf of people and institutions. I submit this comment in my individual capacity and have no financial relationship with any payment stablecoin issuer, custodian or digital asset service provider.

My comment addresses one question that the proposal's risk-management and custody standards do not yet answer directly: when software acting for a customer initiates a payment stablecoin transfer or redemption, what shows that the instruction was within the authority the customer gave? It responds to Questions 106, 110, 117, 124, 126, 128, 163, 181, 187, 193, 239, 246, 249 and 251.

1. A valid transfer is not necessarily an authorized one

A transfer can be backed by compliant reserves, signed with a valid key and recorded correctly on a distributed ledger, and still be one the customer never intended. Consider a business that uses an automated agent to pay an overseas supplier in payment stablecoins. A forged invoice changes the supplier's address. The agent reads the invoice and initiates the transfer, and a signing service approves it under credentials the business granted. The ledger now records a technically valid transfer. What is missing is evidence that the business approved the new beneficiary. No reserve report, however accurate, answers that question.

This is not a risk that only artificial intelligence creates; ordinary credential compromise and weak payment controls can produce the same loss. What changes with automated agents is the speed and reach of software that turns instructions into payments, and its exposure to manipulated inputs. NIST's taxonomy of adversarial machine learning (NIST AI 100-2 E2025, March 2025) describes indirect prompt injection, in which content that an AI system processes, such as a document or web page, carries instructions that change what the system does. An invoice is exactly such content.

The preamble notes that artificial intelligence tools may be used to find and exploit weaknesses in online portals and smart contracts (91 Fed. Reg. at 61610, 61623). A distinct risk arises when automated tools act through valid interfaces on a customer's behalf. The information technology and security standards in proposed § 247.13(b) address private key management, whether smart contracts operate as intended, and the protection of customer records against unauthorized access. These controls are necessary: they secure the means of signing and recording a transaction. They do not by themselves establish that a given instruction fell within the customer's grant of authority, which is

the evidence a customer, an issuer or custodian, and a supervisor will each need when a delegated transaction is disputed.

2. Recommendations

(a) Treat delegated and automated instructions as a named risk area (Questions 110, 124 and 126). Where a Board-supervised permitted payment stablecoin issuer (PPSI) or a Board-supervised custodian executes transfers or redemptions on instructions from automated systems acting for customers, its risk and control framework under proposed § 247.13 should address how it establishes that each instruction falls within the authority the customer granted. This applies equally to a PPSI that holds digital assets on a customer's behalf (see 91 Fed. Reg. at 61611 n.62). A principles-based standard would suffice; the Board need not prescribe a specific technology.

(b) Preserve a record of the payment mandate for consequential delegated transactions (Questions 126 and 128). The record should connect the transfer or redemption to the permission in force when it was initiated: the authorized payer; the intended beneficiary or controlled list of beneficiaries; the asset and network; the maximum amount or exposure; the validity period; and the party responsible for approving exceptions. A change to the beneficiary or to a spending limit should require fresh authorization under the applicable rules. An automated system's explanation of an instruction, or its stated confidence, should not itself expand the mandate. The record should be available to the customer, and to supervisors and investigators as appropriate. To protect customer privacy, it need not be published on a public ledger, and it can be retained off-chain under the record-protection and retention standards in proposed §§ 247.13(b)(5) and 247.14(g).

(c) Clarify custodians' evidence of customer direction (Questions 181, 187 and 193). Proposed Subpart C (§§ 247.20–247.22) defines the custody agreement as one between the covered customer as principal and the custodian as agent (91 Fed. Reg. at 61632), and Question 193 contemplates a custodian that executes and settles at the covered customer's direction. Whether Subpart C remains limited to covered assets as proposed or is extended to all custodied payment stablecoins as Question 181 asks, where instructions reach a covered custodian through an automated intermediary, its written policies, procedures and internal controls under proposed § 247.21(b)(1), and its custody agreements, should identify what evidence establishes that the direction came from the customer and stayed within the terms the customer set.

(d) Carry mandate evidence through service-provider contracts (Questions 124 and 126). Proposed § 247.13(a)(5) would require Board-supervised PPSIs to require their service providers by contract to implement appropriate measures. Question 125 asks about third parties involved in tokenizing reserve assets; the same concern reaches further. Where a provider supplies the software or signing infrastructure that initiates or approves customer transfers or redemptions, those contracts should cover the retention of, and timely access to, mandate records, so that the evidence is not lost between providers when a transaction is disputed.

(e) Make unauthorized-delegation losses visible in operational loss data (Question 163). Under proposed § 247.18(c)(1), Board-supervised PPSIs would map operational losses of at least $20,000 to one of seven event categories consistent with the Basel standard, and would collect descriptive information about the drivers of loss events. Without altering those seven categories, the Board could specify a standard driver tag or sub-classification for losses arising from transactions executed outside verified customer authorization, including through delegated or automated systems. That

classification would let the Board see whether such losses grow as automation spreads, at minimal cost to reporting firms.

(f) Disclose the remedy plainly (Questions 106 and 117). The public disclosures in proposed § 247.12(e), and the customer agreements that must carry them, should also state, in plain language, what remedy, if any, is available when a transfer initiated on the customer's behalf was not authorized, and that settlement on a distributed ledger may be irreversible in practice. A payment stablecoin is not a deposit, and the existence of a freeze or recovery capability does not establish a customer's right to its use. These differences should be clear before money moves, not first explained after it is lost.

(g) Test the dispute, not only the controls (Questions 246 and 251). In periodic independent testing under proposed § 247.13(b)(3) and in examinations under proposed § 247.14, the Board could ask supervised entities that support delegated transactions to demonstrate how they would handle a small set of scenarios: a changed beneficiary on an invoice; a compromised delegated credential; two conflicting instructions; and an interruption during settlement. In each, the questions are whether the customer can establish which mandate was in force, whether the entity can identify the unauthorized change, and how quickly further transactions can be stopped.

3. Scope and proportionality

These recommendations are limited to entities the Board would supervise. They do not ask the Board to regulate self-custody wallet hardware or software excluded under section 10(e) of the Act and proposed § 247.23, or developers of AI systems, beyond its authority under the Act. Small, low-value transactions and supervised business payments do not warrant identical procedures, and much of what is recommended may already be met by the authentication, fraud and dispute practices that banking organizations use today, including within the enterprise-wide risk management that proposed § 247.13(c) contemplates. The case for an explicit standard is strongest where automated systems can move consequential value across several providers, and where ledger settlement offers no built-in chargeback.

Because a single transaction may pass through an issuer, a custodian and service providers supervised by different agencies, I also encourage the Board to coordinate with the OCC, FDIC and NCUA (see Question 239), and with NIST on compatibility and interoperability standards under section 12 of the Act (see Question 249), so that consistent mandate evidence is recognized across supervised institutions.

Thank you for considering these comments.

Respectfully submitted,

Burak Oktenli
Independent Researcher
Washington, DC