RISK FACTOR RESEARCH, LLC, ANDREW G. HUFF

Proposal and Comment Information

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

Comment ID: FR-2026-0033-01-C24

Submitter Information

Organization Name: Risk Factor Research, LLC

Organization Type: Organization

Name: Andrew G. Huff

Submitted Date: 10/22/2026

Re: Implementing the Federal Reserve Board's Responsibilities Under the GENIUS Act; Docket No. R-1899; RIN 7100-AH29; FR Doc. 2026-19860; 91 FR 61580 (September 29, 2026)

I submit the attached comment in my individual capacity; affiliation is for identification only. Dear Mr. McDonough: I am a security engineer and epidemiologist. I was a Senior Member of Technical Staff at Sandia National Laboratories, and I build and test agentic AI systems that read untrusted content. I am not a lawyer or a bank regulator, and I confine these comments to definitions, reserve and reporting design, key custody, and the security program in proposed Sec. 247.13(b). The strongest case for the proposal comes first. One-to-one reserves in cash, Federal Reserve Bank balances, deposits at insured depository institutions, and Treasuries of 93 days or less; a disclosed redemption period of no more than two business days; a monthly composition report; and supervision by a bank regulator with examination machinery already built: that is the right structure for an instrument whose whole value rests on redemption at par on demand. I support the proposal. My recommendations are refinements, and most ask the rule to say in plain words what an examiner can test.

Summary of recommendations: 1. Questions 13 and 4: define nonpublic personal information at least as broadly as the Gramm-Leach-Bliley Act does, and define customer for the privacy standard as any natural person whose data the issuer collects or processes. 2. Questions 20 and 23: define a private key by the ability to authorize a transfer and a holder by control of that credential; state dual control, hardware isolation, and post-quantum readiness for issuer signing keys. 3. Question 24: include decentralized exchange volume in trading volume. 4. Questions 41 and 42: state the reuse prohibition as a flat rule and define the liquidity phrase by a documented stress test. 5. Questions 142, 144, and 139: publish the weekly data in aggregate per stablecoin on a monthly lag, collect secondary market data, adopt the random-day reserve report, and add redemption rates and failed or delayed redemptions to the extended examination cycle factors. 6. Question 126: add a fixed-clock notification requirement for unauthorized access to sensitive customer information, express treatment of smart contracts and encryption, a stated threat model, post-quantum readiness, and a separation rule for AI agents and similar automated systems. 7. Questions 128 and 129: add data minimization, retention, and named sharing destinations to Sec. 247.13(b)(5); require a dependency inventory and contingency for each supported ledger under Sec. 247.13(b)(4).

The full comment is attached as a PDF.

Disclosure: I have no financial interest in any vendor or contract involving this program, and I was not compensated for this comment.

--
Andrew G. Huff, Ph.D., M.S.

Founder
Risk Factor Research, LLC
andrewhuff.com<https://andrewhuff.com>
X (Twitter) @AGHuff<https://twitter.com/AGHuff>
Risk Factor Substack<https://aghuff.substack.com/>

Andrew G. Huff, Ph.D., M.S. **October 22, 2026**
Risk Factor Research, LLC, Michigan, USA
contact@andrewhuff.com

Board of Governors of the Federal Reserve System
Docket No. R-1899; RIN 7100-AH29 (document FR-2026-0033-01 (Board proposal ID); FRS-2026-4226-0001 (regulations.gov mirror))
Federal Register document 2026-19860 (91 FR 61580, September 29, 2026)
Submitted via the Board's web form (Docket No. R-1899; RIN 7100-AH29); comments due November 30, 2026

Re: Implementing the Federal Reserve Board's Responsibilities Under the GENIUS Act; Docket No. R-1899; RIN 7100-AH29; FR Doc. 2026-19860; 91 FR 61580 (September 29, 2026)

Dear Mr. McDonough: I am a security engineer and epidemiologist. I was a Senior Member of Technical Staff at Sandia National Laboratories, and I build and test agentic AI systems that read untrusted content. I am not a lawyer or a bank regulator, and I confine these comments to definitions, reserve and reporting design, key custody, and the security program in proposed Sec. 247.13(b). The strongest case for the proposal comes first. One-to-one reserves in cash, Federal Reserve Bank balances, deposits at insured depository institutions, and Treasuries of 93 days or less; a disclosed redemption period of no more than two business days; a monthly composition report; and supervision by a bank regulator with examination machinery already built: that is the right structure for an instrument whose whole value rests on redemption at par on demand. I support the proposal. My recommendations are refinements, and most ask the rule to say in plain words what an examiner can test.

Summary of recommendations

1. Questions 13 and 4: define nonpublic personal information at least as broadly as the Gramm-Leach-Bliley Act does, and define customer for the privacy standard as any natural person whose data the issuer collects or processes.

2. Questions 20 and 23: define a private key by the ability to authorize a transfer and a holder by control of that credential; state dual control, hardware isolation, and post-quantum readiness for issuer signing keys.

3. Question 24: include decentralized exchange volume in trading volume.

4. Questions 41 and 42: state the reuse prohibition as a flat rule and define the liquidity phrase by a documented stress test.

5. Questions 142, 144, and 139: publish the weekly data in aggregate per stablecoin on a monthly lag, collect secondary market data, adopt the random-day reserve report, and add redemption rates and failed or delayed redemptions to the extended examination cycle factors.

6. Question 126: add a fixed-clock notification requirement for unauthorized access to sensitive customer information, express treatment of smart contracts and encryption, a stated threat model, post-quantum readiness, and a separation rule for AI agents and similar automated systems.

7. Questions 128 and 129: add data minimization, retention, and named sharing destinations to Sec. 247.13(b)(5); require a dependency inventory and contingency for each supported ledger under Sec. 247.13(b)(4).

Questions 13, 4, and 128: the privacy obligation should follow the data

Question 13 asks whether nonpublic personal information should align with the Gramm-Leach-Bliley Act definition and cover any information a customer provides. Question 4 asks whether customer should reach only persons with direct interactions with the issuer or all downstream holders. Issuers process data about people who never signed their terms: a wallet address and its transaction history can be joined to an identity by the issuer, an exchange, or an analytics vendor. If the safeguards in proposed Sec. 247.13(b)(5) attach only to persons with a contract, the people least able to protect themselves are the ones left out. I recommend that the Board define nonpublic personal information at least as broadly as 15 U.S.C. 6809(4) and define customer for purposes of Sec. 247.13(b)(5) as any natural person whose nonpublic personal information the issuer collects or processes. Question 128 asks whether additional data privacy requirements belong in part 247. Three do: collect only the data a stated purpose needs; state a retention period for identifying data; and name the categories of permitted sharing destinations, so that each new destination must be justified.

Questions 20 and 23: a private key is a credential, and custody of it is a security function

Question 20 asks whether private key should refer to a sequence that proves ownership of an account on a distributed ledger. I recommend that the definition turn on capability: a private key is a credential whose possession allows a person to authorize a transfer of a payment stablecoin recorded on a distributed ledger. That wording survives multi-signature and threshold schemes, where no single sequence proves ownership. For Question 23, a payment stablecoin holder should then be the person who controls such a credential, or on whose behalf a custodian controls it.

An issuer's own signing keys control minting, burning, and in many designs freezing, and proposed Sec. 247.13(b)(6) rightly requires measures for private key management, backup, and recovery. NIST has published FIPS 203 and FIPS 204 as post-quantum standards, and NIST IR 8547 proposes deprecating 112-bit-security quantum-vulnerable public-key algorithms after 2030 and disallowing all of them after 2035. I recommend that Sec. 247.13(b)(6) state three expectations for issuer signing keys: dual control, so that no single person can authorize issuance; hardware isolation, so that the complete key never exists in software memory on a networked host; and a documented migration plan to post-quantum signatures and to post-quantum protection of any encryption that guards key material.

Question 24: trading volume should include decentralized exchanges

Question 24 asks whether trading volume should be limited to exchange trades and whether decentralized exchanges should count. They must. Surveillance that counts only centralized exchange volume is blind to venues where a single actor can trade against itself at low cost. On-chain volume is publicly observable, so the impediment is one of method, not access; the Board can name the public data sources and the method issuers must use.

Questions 41 and 42: a clear reuse prohibition and a stated liquidity test

On Question 41, the prohibition against pledging, rehypothecating, or reusing reserve assets should be stated as a flat rule with the collateral trustee case as a disclosed exception. On Question 42, the phrase about creating liquidity to meet reasonable expectations of redemption requests invites a definition in measurement terms: each issuer should run and document a liquidity stress test showing that it can meet a stated share of outstanding issuance, redeemed within the two-business-day period, from cash and overnight instruments without selling Treasuries into a falling market. Pre-approval of term repurchase agreements in stress is reasonable if bounded by that test. Risk is likelihood times consequence; the consequence of a missed redemption window can be a run, and the test is what puts a number on the likelihood.

Questions 142, 144, and 139: publish the vital signs

Proposed Sec. 247.14(h) requires a confidential weekly report per stablecoin on issuance, redemption, trading volume, and reserves. Question 142 asks whether the data should be made public and on what timeframe. Yes. The asset being regulated here is public confidence, and confidence is sustained by data the public can read, not only by data the supervisor holds. I recommend that the weekly data be published in aggregate form, per stablecoin, on a monthly lag, including redemption volume and times and reserve composition, with a count of failed or delayed redemptions. The lag and the aggregation keep the series from serving as a run signal. The Board should also collect secondary market price and volume data; manipulation shows up there first. On Question 144, I support a published reserve composition report as of a day randomly selected each month by the issuer's registered public accounting firm, because an unpredictable date is a cheap audit control. On Question 139, the extended examination cycle under Sec. 247.14 should adopt redemption rates, which the question suggests, and add the count of failed or delayed redemptions; they are the earliest signals of a weakening promise.

Questions 126 and 129: the information technology and security program

Proposed Sec. 247.13(b)(2) through (b)(6) require board oversight, an asset inventory, controls for sensitive information, validation of key systems including smart contracts, testing, incident response, continuity planning with due diligence before supporting a new ledger, safeguards for nonpublic personal information, and secure handling of private keys. That is a sound frame. Question 126 asks what is omitted, and I recommend four additions. First, a notification requirement for unauthorized access to sensitive customer information on a fixed clock, as the OCC proposed; the banking agencies' computer-security incident notification rule already uses 36 hours. Second, express treatment of smart contracts and encryption: an issuer should state which contract functions can mint, burn, freeze, or upgrade, and which algorithms protect the keys that control them. Third, a written threat model naming the adversaries defended against, including key theft, insider misuse, and compromise of the systems that process redemptions, with the post-quantum readiness described above. Fourth, a plain-words separation rule for AI agents and other automated systems that interpret free-form content. Any such system that reads untrusted content, holds customer data or key material, and can transmit or transact holds all three elements of what practitioners call the lethal trifecta, and I have built enough of these systems to say that the failure is ordinary: content written by an adversary becomes an instruction. The rule should require that, for such systems, those three capabilities never sit in one component and that every machine-proposed transaction remain a candidate until a human or an isolated policy engine accepts it.

Question 129 asks about risks from the blockchains on which the coins circulate. An issuer's security depends on ledgers it does not control: a consensus failure, a chain reorganization, or a governance change on a supported ledger can halt redemptions or duplicate supply with no fault on the issuer's part. Consistent with the due diligence and continuity duties in Sec. 247.13(b)(4), the rule should require a stated dependency inventory and a written contingency for each supported ledger, including when the issuer would halt issuance on that ledger.

Scope and confidence

This comment addresses Questions 4, 13, 20, 23, 24, 41, 42, 126, 128, 129, 139, 142, and 144. I reviewed the definitions, activities, risk management, and reporting preamble; I did not review the capital, custody, tying, State-qualified issuer, or economic analysis sections, and I defer to counsel on statutory authority. My confidence is high that issuer signing keys are the controlling security asset and need stated custody and post-quantum expectations; high that the privacy definition should follow the data; moderate to high that a lagged public series would improve stability more than it costs; and moderate on the form of the liquidity stress test.

Disclosure: I have no financial interest in any vendor or contract involving this program, and I was not compensated for this comment.

Thank you for the opportunity to comment.

Respectfully,

Andrew G. Huff, Ph.D., M.S.
Risk Factor Research, LLC

References

1. Board of Governors of the Federal Reserve System, Implementing the Federal Reserve Board's Responsibilities Under the GENIUS Act, notice of proposed rulemaking, 91 FR 61580, September 29, 2026, https://www.federalregister.gov/documents/2026/09/29/2026-19860

2. GENIUS Act, Pub. L. 119-27 (July 18, 2025), 12 U.S.C. 5901 et seq., https://www.congress.gov/bill/119th-congress/senate-bill/1394

3. 15 U.S.C. 6809, Definitions (Gramm-Leach-Bliley Act), https://www.law.cornell.edu/uscode/text/15/6809

4. National Institute of Standards and Technology, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203, August 2024, https://doi.org/10.6028/NIST.FIPS.203

5. National Institute of Standards and Technology, Module-Lattice-Based Digital Signature Standard, FIPS 204, August 2024, https://doi.org/10.6028/NIST.FIPS.204

6. National Institute of Standards and Technology, Transition to Post-Quantum Cryptography Standards, NIST IR 8547 (initial public draft), November 2024, https://doi.org/10.6028/NIST.IR.8547.ipd

7. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, January 2023, https://doi.org/10.6028/NIST.AI.100-1

8. Willison S, The lethal trifecta for AI agents: private data, untrusted content, and external communication, June 16, 2025, https://simonwillison.net/2025/Jun/16/the-lethal-trifecta/