MICHAL NIEMIEC

Proposal and Comment Information

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

Comment ID: FR-2026-0033-01-C28

Submitter Information

Name: Michal Niemiec

Submitted Date: 10/30/2026

Please see the attached comment letter from Michal Niemiec on Docket No. R-1899 (RIN 7100-AH29) and Docket No. R-1900 (RIN 7100-AH30). The same letter is being submitted on both dockets.

October 30, 2026

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

Submitted via the Board's website (https://www.federalreserve.gov/apps/proposals/)

Re: (1) Implementing the Federal Reserve Board's Responsibilities Under the GENIUS Act, Docket No. R-1899; RIN 7100-AH29 (91 FR 61580, September 29, 2026); and (2) Application Procedures for Board-Supervised Insured Depository Institutions Seeking Approval for a Subsidiary To Issue Payment Stablecoins, Docket No. R-1900; RIN 7100-AH30 (91 FR 61346, September 29, 2026)

Dear Mr. McDonough:

1. Introduction and background

I appreciate the opportunity to comment on the Board's proposed Regulation UU (12 CFR part 247) and the related application procedures proposed in Docket No. R-1900. I submit this comment in my individual capacity, drawing on nearly 14 years of experience in lending. I spent years leading teams that built B2B lending products. I am the founder of Stone and Pebble Consulting LLC, an early-stage firm that may in the future offer services to banks or their third parties; this comment reflects my own views and does not promote any product.

Summary of requests

#	Request	Proposed section	Board question(s)	Letter §
1	Coordinate with FinCEN so that permitted CIP reliance, or a verifiable credential acceptable under FinCEN's proposed CIP rule (91 FR 37234), once final, counts toward § 247.12(d) and is not by itself a reason for additional redemption time	§ 247.12(b)(2), (d)	Q97–Q99	4
2	Confirm that privacy-preserving attestations of reserve composition may supplement, but not replace, the monthly report and accounting firm examination	§ 247.11(d)–(e)	Q84, Q88–Q91, Q144, Q145	5
3	State that "material" service providers include those that never touch customer data	§ 247.13(a)(5)	Q125, Q126	6
4	Add data minimization to the nonpublic-personal-information safeguards	§ 247.13(b)(5)	Q128	6
5	Align BSA/sanctions expectations with FinCEN and the other agencies	§ 247.13(d)	Q134, Q137	7
6	Custody: segregation evidence for omnibus accounts, and prompt release for redemption	Subpart C	Q187, Q191, Q193	8
R-1900 (asks 1, 3, 6)	Read "material third-party relationships" to include providers that never touch customer data; policies should address how CIP reliance and redemption timing interact	R-1900 § 247.30(b)(2)(i)(D), (b)(2)(iii)	R-1900 Q10	9

#	Request	Proposed section	Board question(s)	Letter §
R-1900 (asks 2, 6)	Reserve evidence covers the month-end examination, any supplemental attestations, and custody arrangements	R-1900 § 247.30(b)(2)(ii)–(iii)	R-1900 Q11	9
R-1900 (asks 1, 2, 5)	Streamlining: cross-reference existing CIP/BSA policies and the § 247.11 reporting plan	R-1900 § 247.30(b)(2)	R-1900 Q15	9

2. The strongest objection, and my response

The strongest objection comes from another docket. In a comment on the SEC's Regulation Crypto Assets proposal, another commenter, the Independent Community Bankers of America, noted that "Crypto growth may migrate transactional balances from community banks to stablecoin issuers, …" and that "Community banks then lose both stable funding and the customer payment relationship, increasing funding costs and reducing lending capacity." (ICBA, Comment on File No. S7-2026-27, Oct. 20, 2026, at 2 and 4, https://www.sec.gov/comments/S7-2026-27/s7202627-1100619-3879786.pdf). On that view, easier redemption or verification could speed deposit flight.

I take that concern seriously; local deposits are an important source of funding for local credit. But my requests do not expand what a permitted payment stablecoin issuer may do, and they leave untouched the limits on paying remuneration to holders (proposed § 247.10(c)(4); Q38, 91 FR 61593), a principal way the proposal limits deposit-like competition. Most concern how facts the Board already requires are verified; Requests 3 and 4 add targeted oversight and data-minimization expectations. Federal Reserve research also suggests the effect is not one-directional: "Stablecoins can either reduce, recycle, or restructure bank deposits rather than simply draining them" (J. Wang, "Banks in the Age of Stablecoins: Some Possible Implications for Deposits, Credit, and Financial Intermediation," FEDS Notes, Dec. 17, 2025, § 2, https://www.federalreserve.gov/econres/notes/feds-notes/banks-in-the-age-of-stablecoins-implications-for-deposits-credit-and-financial-intermediation-20251217.html). Redemption can be one path by which funds return to bank deposits, so delaying it may not protect community banks. Even so, recycled deposits need not return to the community bank that lost them, and these requests do not resolve that concern; they seek proportionate verification, oversight, and privacy protections while preserving the statutory safeguards.

The point that verification can be separated from data collection is not new. Then-Commissioner Hester M. Peirce said: "Cryptography allows us to be confident that a fact is true without knowing the underlying data." (Remarks before SIFMA's Digital Assets Conference, Sept. 23, 2026, https://www.sec.gov/newsroom/speeches-statements/peirce-looking-change-haystacks-remarks-sifma-s-digital-assets-conference-092326; her own views, not the Commission's.) I cite her only for the general point that privacy-enhancing technologies, of which zero-knowledge proofs are one example, can help protect personal data. I do not suggest that any technology reduces or replaces customer identification, BSA/AML, sanctions, or recordkeeping obligations.

Other commenters have raised related points, including data minimization (R-1899 Comments C07, C17, and C24); narrower use of redemption-delay exceptions, a labeled preliminary reserve snapshot, and the limits of technical proofs of assets (C07); how lawful reviews affect the redemption clock, and labeling of pre-examination reports (C03); supporting evidence for the reserve report and examination (C18); the materiality of providers based on their function (C17); access to and release of reserve assets held in custody (C03 and C25); not duplicating FinCEN and OFAC requirements (C19); and reuse of existing records in applications (R-1900 Comments C03, C09, and C12). I am not affiliated with these commenters and cite them only to note that these points appear in the record.

3. Scope

I answer selected questions on customer identification and redemption timing, reserve reporting and attestations, third parties and data privacy, BSA/AML and sanctions alignment, custody, and the R-1900 application procedures; Appendix A lists them, and I offer no comment on the rest.

4. Redemption timing and customer verification (§ 247.12; Q97–Q99)

Q97 (91 FR 61605). Two business days is a reasonable outer limit for a customer whose identity is already verified. The Board recognizes that reviews for customers without pre-existing relationships may take longer (91 FR 61605), which is where coordination can help.

Q98 (91 FR 61605). Start the clock at the request, as proposed. The § 247.12(d) safe harbor already covers verification delays; starting only after customer identification is complete would let slow verification extend redemption time without limit. The OCC's final rule starts the clock after onboarding only where an issuer's onboarding procedures are "reasonably designed to not unduly delay the onboarding of retail or other customers, including in times of stress" (12 CFR 15.12(a)(1)(ii), 91 FR 67181), so that onboarding cannot be used "as a pretext to artificially extend the timeline for redemption" (91 FR 67065). Because the joint CIP proposal would apply to Board- and OCC-supervised issuers (91 FR 37235), permitted reliance offers a common way to keep onboarding from delaying redemption.

Q99 (91 FR 61605). The safe harbor is appropriately scoped and properly conditioned on the issuer "demonstrating that it has made all reasonable efforts to resolve the delay" (proposed § 247.12(d), 91 FR 61673). The Board should clarify which verification already satisfies it, so it does not become a routine extension.

Coordination on customer verification (Questions 97–98). Proposed § 247.12(d) would excuse a failure to redeem on time where additional time is needed for customer identification and due diligence (91 FR 61605). The joint customer identification program proposal would permit reliance on another regulated financial institution's CIP (proposed 31 CFR 1033.220(a)(6)), and it acknowledges interest in verifiable credentials and digital identity (91 FR 37242). I respectfully ask the Board to coordinate with FinCEN so that permitted reliance, or a verifiable credential acceptable under that rule, satisfies the verification that § 247.12(d) contemplates, consistent with the issuer's BSA/AML, sanctions, and CIP obligations under FinCEN's rule, once final, so that customer identification already completed in that way does not by itself support additional time under § 247.12(d)(i) (91 FR 61673). This would not limit risk-based due diligence, current sanctions screening, or checks prompted by suspected fraud or changed information. FinCEN has not proposed regulatory text on verifiable credentials (91 FR 37242), so that part of Request 1 would apply only to the extent the final CIP rule or FinCEN accepts them.

The Board's stated reason for the identification prong is that "customer identification and due diligence reviews for customers without pre-existing relationships with Board-supervised PPSIs may take longer than two days" (91 FR 61605). Where identification has already been completed through permitted reliance, that reason does not apply to the identification step, although it may still apply to due diligence. The statute requires each issuer's redemption policy to "establish clear and conspicuous procedures for timely redemption of outstanding payment stablecoins" (12 U.S.C. 5903(a)(1)(B)(i)); counting completed identification once serves that requirement without relaxing any identification duty. One objection is that reliance weakens identification. The joint CIP proposal answers much of it: reliance must be "reasonable under the circumstances," the relied-upon institution must be federally regulated and subject to CIP requirements, it must certify annually by contract, and the issuer "would remain responsible for its compliance" (91 FR 37243). Request 1 asks only that identification

completed under those conditions count once. Reusing completed verification in this way could also help issuers confirm identity without collecting or copying more personal data than necessary. The joint CIP proposal asks whether it should account for "situations where a customer's only desired relationship with a PPSI is to redeem a payment stablecoin" (91 FR 37244). Coordinating the answer to that question with § 247.12(d)(i) would help ensure that one agency's identification rule and the other's redemption timeline produce a single, predictable expectation for holders.

For example, suppose a holder whose identity a federally regulated bank has verified under its CIP asks a Board-supervised PPSI to redeem on a Monday, and the PPSI's CIP permits reliance on that bank under proposed 31 CFR 1033.220(a)(6). Under Request 1, the PPSI would not ordinarily cite customer identification under § 247.12(d)(i) to pay after Wednesday. If sanctions screening returned a potential match, or the holder's information had changed, § 247.12(d)(i) would remain available for that review.

Insert-ready text (§ 247.12(d)):

> "For purposes of paragraph (d)(i), a Board-supervised PPSI that has verified a customer's identity in accordance with 31 CFR part 1033, including through permitted reliance on another financial institution or through other means acceptable under that part, should not ordinarily require additional time for customer identification in connection with that customer's redemption request."

5. Reserve reporting and attestations (§ 247.11(d)–(e); Q84, Q88–Q91, Q144, Q145)

Proposed § 247.11(e)(1) requires that the monthly report "must have been examined by a registered public accounting firm prior to publication" (91 FR 61672).

- **Q88 (91 FR 61602):** Yes. Use a fixed month-end time, consistent with the 5:00 p.m. daily valuation in § 247.11(a)(2) (Q48, 91 FR 61596).
- **Q89 (91 FR 61602):** Yes. Publish the certification with the report.
- **Q90 (91 FR 61602):** No. Unexamined figures invite confusion if later revised.
- **Q91 (91 FR 61602):** Largely clear. I support an examination at the reasonable-assurance level, using as criteria the reserve requirements in § 247.11(a) and (b) as of the report date (91 FR 61671), and supported by evidence beyond management's assurances alone. I take no position on the engagement-letter compliance attestation, and I do not suggest that a supplemental attestation could serve as that examination. Because § 247.11(a)(1)(iii) applies at all times, the random-date report I support under Q144 would complement these month-end criteria.
- **Q84 (91 FR 61601):** Let issuers optionally publish privacy-preserving attestations that help holders confirm the report matches the issuer's records, as a supplement to, never a replacement for, the accounting firm's examination. In a comment on the SEC's Regulation Crypto Assets proposal, another commenter noted: "That data should be backed by monthly independent attestation and an annual audit." (Keystone Technology Group, Comment on File No. S7-2026-27, at 12, https://www.sec.gov/comments/S7-2026-27/s7202627-1084099-3777547.pdf). Any such attestation should state its as-of date, the records and populations of assets and liabilities it covers, and its limitations, and should not imply assurance about legal ownership, encumbrances, completeness of liabilities, or continuing availability unless those matters are within its stated scope. Any such attestation should also state that it is not the examination required by § 247.11(e).
- **Q145 (91 FR 61616):** To limit duplication, the Board should let the monthly reserve examination under § 247.11(e) (12 U.S.C. 5903(a)(3)(A)) and any annual audit required by proposed § 247.14(l) draw on the same underlying evidence, while preserving each engagement's scope, standards, and access to records. I support placing in the rule text the framework the Board describes at 91 FR 61615–61616: that

"applicable auditing standards" for the annual audit (12 U.S.C. 5903(a)(10)(A)(iii)) are those that would apply under section 13(a) or 15(d) of the Securities Exchange Act of 1934, that the Board enforces them, and that the accounting firm must provide requested information and working papers. Each engagement should document its own evidence and conclusions; shared evidence should reduce duplicate requests, not lead one engagement to rely on the other's conclusions.

- **Q144 (91 FR 61615):** I support a random test date chosen by the accounting firm and disclosed afterward. The OCC did not require a random-date attestation in its final rule but noted that issuers "may, nevertheless, decide to engage in random-day reporting and certification as a best practice" (91 FR 67060); the Board could recognize the same practice.

Insert-ready text (§ 247.11(e)):

> "(3) Nothing in this paragraph prohibits a Board-supervised PPSI from publishing additional attestations or verification tools relating to its reserve assets, provided that such materials do not replace, and are not inconsistent with, the report and examination required by paragraphs (d) and (e)(1) of this section."

6. Material vendors and data privacy (§ 247.13(a)(5), (b)(5); Q125, Q126, Q128)

Proposed § 247.13(a)(5) requires an issuer to "exercise appropriate due diligence in its third party relationships" and to monitor them "as appropriate … including by reviewing audits, summaries of test results, or other equivalent evaluations" (91 FR 61673). The preamble notes providers may "support the development of smart contract code that facilitates the burning, minting, transferring or other functions of payment stablecoins" (91 FR 61608).

Q125 (91 FR 61610), Q126 (91 FR 61611): A provider can be material without receiving customer data: smart-contract code, reserve-asset tokenization, reserve valuation, blockchain monitoring, issuance and transfer agents, attestation providers. Where diligence focuses on data access, these may receive less review than their importance warrants. The 2023 interagency guidance already defines critical activities by effect, as those that could "Cause a banking organization to face significant risk if the third party fails to meet expectations" or "Have a significant impact on a banking organization's financial condition or operations" (Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920, 37927 (June 9, 2023); the guidance is not a binding regulation). The Board should say materiality turns on a provider's effect on issuance, redemption, reserves, or compliance, not only data access, and that issuers relying on a provider's attestations should confirm their scope and period cover the services used.

Q128 (91 FR 61611): Proposed § 247.13(b)(5) requires safeguards to "ensure the security and confidentiality of records containing nonpublic personal information about a customer" (91 FR 61674). I recommend a data-minimization principle: where an issuer or provider needs only to confirm a fact (for example, that a customer is verified or not sanctioned), it should prefer methods, including verifiable credentials or privacy-preserving attestations, that confirm the fact without spreading copies of records. This would not override recordkeeping under 31 CFR chapter X; the joint CIP proposal would require identifying information to be retained "for five years after the date the account is closed" (proposed 31 CFR 1033.220(a)(3), 91 FR 37243). The OCC took a similar case-by-case view in its final rule, stating that whether a privacy-enhancing architecture can meet both its safeguards and BSA/AML requirements "will depend on the facts of that particular architecture" (91 FR 67076). That supports treating these methods as a supplement to, not a replacement for, required records.

Insert-ready text (§ 247.13(a)(5)):

"(iv) identify service providers whose failure could materially affect issuance, redemption, reserve assets, or compliance with this part, whether or not such providers receive nonpublic personal information, and apply oversight commensurate with that effect."

Insert-ready text (§ 247.13(b)(5)):

"(v) limit the collection, sharing, and retention of nonpublic personal information to what is reasonably necessary, consistent with applicable recordkeeping requirements."

7. BSA/AML and sanctions alignment (§ 247.13(d); Q134, Q137)

Q134 (91 FR 61612): Yes. Include provisions similar to the FinCEN notice-and-consultation and information-sharing provisions the OCC, FDIC, and NCUA have proposed (91 FR 37840; 91 FR 34171; 91 FR 28956), so that FinCEN is consulted on AML/CFT enforcement actions and significant AML/CFT supervisory actions in the same way whichever agency supervises the issuer. I take no position between the two information-sharing options described in those proposals. The OCC finalized its GENIUS Act rule on October 21, 2026, effective January 18, 2027, and will address BSA/AML and sanctions in a separate rulemaking (91 FR 67000, 67001). I ask the Board to keep its requirements aligned with that final rule where the statute permits. **Q137 (91 FR 61612):** I support the Board's stated approach that compliance with 31 CFR Chapters V and X would constitute compliance with § 247.13(d) (91 FR 61612), while preserving the Bank Secrecy Act and GENIUS Act section 4(a)(5) and (a)(6) obligations named in proposed § 247.13(d)(2) (91 FR 61674). Where other Board BSA, sanctions, or suspicious-activity rules also apply, the Board should identify them and resolve any conflict in favor of a single set of expectations.

8. Custody and segregation (Subpart C; Q187, Q191, Q193)

Q187 (91 FR 61634), Q191 (91 FR 61635): For omnibus accounts, a custodian should be able to show at any time each covered customer's entitlement and that the omnibus balance covers all of them, without disclosing other customers' balances. **Q193 (91 FR 61635):** Yes. Custody agreements should provide for prompt release of covered assets so the two-business-day standard in § 247.12(b)(2) can be met.

9. Application procedures (Docket No. R-1900)

R-1900 Q10 (91 FR 61352). The required policies are sound. They cover "(A) redemption; (B) maintenance of required reserve assets; (C) custody of customer assets; (D) recordkeeping, reconciliation, and transaction processing; and (E) compliance with Bank Secrecy Act, sanctions compliance program, anti-money laundering, and countering the financing of terrorism requirements" (R-1900 proposed § 247.30(b)(2)(iii), 91 FR 61359). Consistent with Requests 1, 3, and 6, I ask the Board to clarify that "any material third-party relationships" (§ 247.30(b)(2)(i)(D), 91 FR 61359) includes providers whose failure could materially affect issuance, redemption, or reserves even if they never receive customer information, and to consider asking that redemption and BSA policies describe how customer identification, including reliance, interacts with the redemption timeline.

R-1900 Q11 (91 FR 61352). On what best demonstrates "the appropriate composition, custody, and valuation of the reserve assets," and consistent with Requests 2 and 6, applicants should describe (i) how the monthly report will be prepared and examined by a registered public accounting firm; (ii) any supplemental attestations, which would not replace that

examination; and (iii) how custodians will segregate covered assets and release them promptly for redemptions.

Because proposed § 247.11(a)(1)(iii) requires full reserve coverage "at all times" (91 FR 61671), reserve management plans under § 247.30(b)(2)(ii)(C) could also describe how reserve sufficiency will be verified on an ongoing basis after approval.

R-1900 Q15 (91 FR 61353). Consistent with Requests 1, 2, and 5, I ask the Board to consider whether applicants could (i) cross-reference customer identification and BSA/sanctions policies prepared under applicable requirements of 31 CFR Chapters V and X (including, once final, the proposed CIP rule at 91 FR 37234), rather than restating them; and (ii) describe reserve reporting by reference to the monthly report and accountant examination under proposed § 247.11(d)–(e), noting any supplemental attestations separately.

10. Conclusion

These requests are narrow. The central request is simple: identification completed once under applicable CIP rules should count once for redemption timing, while due-diligence, sanctions, fraud, and changed-information reviews remain unaffected. Thank you for your consideration.

Respectfully submitted,

Michal Niemiec

Appendix A: Questions answered

- **R-1899 answered:** Q84, Q88–Q91, Q97–Q99, Q125, Q126, Q128, Q134, Q137, Q144, Q145, Q187, Q191, Q193 (Q38 and Q48 cited only). No comment on the other R-1899 questions (Q1–Q254).
- **R-1900 answered:** Q10, Q11, Q15. No comment on Q1–Q9, Q12–Q14, Q16–Q23.