Public Comment on NCUA Proposed Rule — GENIUS Act Implementation for Federally Insured Credit Unions

Submitted by: Empty Set LLC (Nevada Series LLC) **Contact:** Brice Love, Co-Founder **Email:** brice@emptysetllc.com **Date:** March 10, 2026 **Re:** Proposed Rule — Investments in and Licensing of Permitted Payment Stablecoins Issuers, 91 FR 6531 (February 12, 2026), Docket No. NCUA-2025-1335, RIN 3133-AF69 **Submitted via:** Regulations.gov, https://www.regulations.gov/docket/NCUA-2025-1335

Executive Summary

Empty Set LLC respectfully submits this comment in response to the National Credit Union Administration's proposed rule implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act") for federally insured credit unions. We write to address an issue that is particularly acute for credit unions: the behavioral safety of AI systems that credit unions will rely upon — overwhelmingly through third-party vendors — to comply with the Act's BSA/AML, reserve management, and consumer protection requirements.

Credit unions face a structural challenge that distinguishes them from national banks and large state-chartered institutions. The median federally insured credit union lacks the internal technology staff, model risk management capacity, and examination resources to develop, deploy, or independently validate AI systems for stablecoin compliance. Credit unions entering stablecoin activities will depend almost entirely on third-party vendors for the AI systems that perform transaction monitoring, sanctions screening, suspicious activity detection, reserve management, and consumer disclosure functions.

This vendor dependency creates a compounding risk. The NCUA's examination authority over third-party vendors is limited. Credit unions cannot independently validate the behavioral safety of AI systems whose architectures are proprietary. And the emerging insurance market for AI-related liabilities — reshaped by the January 2026 ISO generative AI exclusions — is pricing AI risk in ways that disadvantage institutions without demonstrable AI governance programs.

The result is that the institutions least equipped to manage AI behavioral risk are the ones most exposed to it.

Empty Set LLC operates a standards development initiative focused on behavioral safety credentialing for autonomous AI agents, with emphasis on the insurance and financial services sectors. We propose that the NCUA incorporate third-party behavioral safety credentialing into the GENIUS Act implementing regulations as a cost-effective, scalable mechanism that allows credit unions to verify the safety of vendor-provided AI systems without requiring in-house model risk management capabilities that most credit unions do not have and cannot afford to build.

I. The Credit Union AI Dependency Problem

A. Resource Asymmetry

The NCUA supervises approximately 4,600 federally insured credit unions. The vast majority are community institutions with total assets under $500 million. These credit unions serve 140 million

members, many in underserved communities where credit unions are the primary or sole financial institution.

For these institutions, stablecoin activities under the GENIUS Act represent both an opportunity and an operational challenge. The opportunity is real: stablecoins can reduce cross-border remittance costs, enable faster settlement, and provide members with access to digital asset services that were previously available only through fintech platforms or large banks. The operational challenge is equally real: compliance with the GENIUS Act's BSA/AML, reserve attestation, and consumer protection requirements demands technological capabilities that most credit unions do not possess internally.

The result is predictable. Credit unions will procure AI-powered compliance solutions from a concentrated set of third-party vendors — the same core processing platforms (Fiserv, Jack Henry, Corelation, Symitar) and specialty compliance vendors (Verafin, NICE Actimize, Abrigo) that already dominate credit union technology. These vendors will deploy AI systems that monitor stablecoin transactions, flag suspicious activity, generate SARs, manage reserves, and produce regulatory reports on behalf of credit unions.

The credit union's compliance obligation is non-delegable. The vendor performs the function; the credit union bears the regulatory consequence if the function is performed poorly. This creates a fundamental disconnect: the institution accountable for compliance has the least visibility into the behavioral characteristics of the AI systems performing that compliance.

B. The NCUA Examination Gap

The NCUA's ability to examine third-party vendors is structurally limited compared to the OCC's authority over bank service providers under the Bank Service Company Act. While the NCUA has interagency coordination arrangements and can request vendor documentation through the credit union, it cannot unilaterally compel a vendor to submit to behavioral safety examination of its AI systems.

This limitation matters because AI behavioral safety is not observable from the credit union's side of the vendor relationship. A credit union can review a vendor's marketing materials, read its SOC 2 report, and monitor the system's outputs. It cannot independently assess whether the AI system's false-positive rates vary by demographic group, whether the system exhibits behavioral drift over time, whether the system is robust to adversarial inputs, or whether the system's training data contains biases that produce discriminatory outcomes.

Third-party behavioral safety credentialing addresses this gap by placing the evaluation burden on an independent credentialing body rather than on the credit union or the NCUA. The credentialing body evaluates the vendor's AI system against defined behavioral safety standards and issues a verifiable credential that the credit union, the NCUA, and the credit union's insurer can all rely upon — without requiring any party to access the vendor's proprietary model architecture.

II. The Community Impact Dimension

Credit unions exist to serve their members, and their members are disproportionately drawn from communities that are most vulnerable to AI behavioral safety failures in financial compliance.

A. Discriminatory False Positives in BSA/AML

The most significant behavioral safety risk in AI-driven BSA/AML compliance is discriminatory false-positive generation — the systematic misidentification of legitimate transactions as suspicious, with disproportionate impact on specific demographic groups or geographic regions.

This risk is not theoretical. Traditional BSA/AML transaction monitoring systems are known to produce higher false-positive rates for cash-intensive small businesses, remittance-heavy corridors, and communities with informal banking practices — patterns that correlate with minority, immigrant, and low-income communities. AI systems trained on this historically biased data inherit and amplify these patterns.

For credit unions, which serve precisely these communities, the consequences of deploying AI systems with unaudited bias characteristics are severe:

- **Member harm**: A stablecoin transaction blocked by a false-positive SAR alert causes immediate financial disruption — failed payments, missed settlement, reputational exposure in transparent blockchain networks.
- **De-risking pressure**: Credit unions with elevated SAR filing rates face examiner scrutiny that can lead to risk-averse decisions to exit stablecoin services entirely — depriving members of access to digital financial services.
- **Community trust erosion**: Credit unions operate on a cooperative trust model. Members who experience AI-driven transaction blocks may perceive the credit union as hostile or discriminatory, undermining the relationship that is the credit union's core competitive advantage.

The NCUA's implementing regulations should require that AI systems used for stablecoin BSA/AML compliance undergo regular demographic impact audits. Credit unions cannot perform these audits themselves — but they can require, as a condition of vendor contracts, that their vendors obtain behavioral safety credentials from independent bodies that include demographic impact testing in their evaluation methodology.

B. The Unbanked and Underbanked Population

The FDIC's most recent survey estimates that approximately 4.5% of U.S. households are unbanked and an additional 14.1% are underbanked. Credit unions serve a disproportionate share of this population. Stablecoin services, if implemented with adequate consumer protections, could expand financial access for these members.

However, AI systems that perform identity verification, transaction monitoring, and risk scoring for stablecoin services may systematically disadvantage the same populations credit unions aim to serve — thin-file consumers, recent immigrants, gig economy workers, and individuals with non-traditional financial patterns. Behavioral safety credentialing that includes fairness testing across these demographic dimensions is essential to ensuring that AI-enabled stablecoin services expand financial inclusion rather than creating a new vector for exclusion.

III. The Insurance and Capital Implications

Credit unions face the same AI liability insurance transformation that is affecting the entire financial sector. The January 1, 2026 ISO endorsements — CG 40 47 (Artificial Intelligence Exclusion),

CG 40 48 (Limited Coverage), and CG 35 08 (Amendatory) — are being adopted across the property-casualty market. These endorsements exclude or restrict coverage for liabilities arising from generative AI systems under standard commercial general liability policies.

For credit unions, the implications are threefold:

Coverage contraction. Credit unions that deploy AI systems for stablecoin operations — or rely on vendors that deploy such systems — will find that AI-related operational liabilities are increasingly excluded from their commercial insurance policies. This coverage gap must be filled either by affirmative AI liability policies (which require demonstrable AI governance) or by self-insurance reserves.

Capital impact. The NCUA's risk-based capital framework does not currently require credit unions to hold capital specifically against AI operational risk. As AI systems take on more consequential compliance functions, and as insurance coverage for AI-related liabilities contracts, the implicit operational risk exposure on credit union balance sheets grows. Behavioral safety credentialing provides the governance evidence that insurers need to offer affirmative coverage — reducing the uninsured operational risk that would otherwise require capital allocation.

Vendor concentration risk. If the handful of core processors serving credit unions deploy AI systems with unexamined behavioral safety characteristics, a single behavioral safety failure — a systematic bias, a training data contamination event, an adversarial exploit — could simultaneously affect thousands of credit unions. This is a systemic risk that the NCUA should address in its GENIUS Act regulations through vendor AI governance requirements.

IV. The Treasury FS AI RMF and Credit Union Proportionality

The Treasury Financial Services AI Risk Management Framework, published February 19, 2026, establishes 230 control objectives for AI governance in financial services. The framework is comprehensive, rigorous, and appropriate for large, sophisticated institutions with dedicated model risk management teams.

It is not, in its current form, proportionate to the resources and capabilities of most credit unions.

The NCUA faces a calibration challenge: the behavioral safety standards for AI systems in stablecoin operations should be rigorous regardless of the institution's size, because the risk to members from AI behavioral failures is not proportional to the institution's asset size. A discriminatory false-positive that blocks a member's stablecoin transaction is equally harmful whether the credit union has $50 million or $50 billion in assets.

Third-party behavioral safety credentialing resolves this proportionality problem. The credentialing standard is applied to the AI system, not to the institution deploying it. A small credit union using a credentialed AI system from its core processor receives the same behavioral safety assurance as a large credit union — without needing to build internal MRM capacity to replicate the evaluation. The cost of credentialing is borne by the vendor (who spreads it across its entire customer base) rather than by each individual credit union.

This is analogous to how credit unions currently manage information security risk. Most credit unions do not maintain internal penetration testing teams. They require their vendors to obtain SOC 2 attestations, and they rely on those attestations for their vendor due diligence obligations.

Behavioral safety credentialing applies the same logic to AI systems: the credit union requires the credential, the vendor obtains it, and the NCUA examiner can verify it.

V. Specific Recommendations

Empty Set LLC recommends the following additions to the GENIUS Act implementing regulations for federally insured credit unions:

1. Require Vendor AI Governance as a Condition of Stablecoin Activity

Credit unions engaging in stablecoin activities should be required to verify that their third-party AI vendors maintain AI governance programs consistent with the Treasury FS AI RMF. The NCUA should specify that acceptable evidence of vendor AI governance includes behavioral safety credentials issued by qualified independent bodies.

2. Recognize Behavioral Safety Credentialing as a Proportionate Compliance Mechanism

The proposed rule should explicitly recognize third-party behavioral safety credentialing as a mechanism by which credit unions can satisfy their AI governance obligations for stablecoin operations. This recognition should include:

- A defined set of behavioral safety standards that credentials must address (error rate tolerance, demographic impact, behavioral drift, human override, adversarial robustness)
- Criteria for qualifying credentialing bodies (independence, technical competence, consistency with NIST AI RMF and ISO 42001)
- Time-limited credentials subject to renewal and revocation upon material safety failures

3. Require Demographic Impact Auditing in Vendor Contracts

Credit unions should be required to include contractual provisions requiring their stablecoin AI vendors to conduct regular demographic impact audits of AI systems used for BSA/AML compliance, identity verification, and risk scoring. Results should be available to the credit union's board and to NCUA examiners upon request.

4. Develop Credit Union-Specific AI Examination Procedures

The NCUA should develop supplemental examination procedures for evaluating credit unions' AI governance in stablecoin operations. These procedures should be calibrated to the credit union model — focusing on vendor credential verification, board oversight of AI risk, and member impact monitoring rather than on internal model development and validation capabilities that most credit unions do not possess.

5. Address Vendor Concentration Risk

The NCUA should assess the concentration of AI-powered stablecoin compliance solutions among credit union service organizations (CUSOs) and core processors. Where a single vendor's AI system serves a significant share of federally insured credit unions, the NCUA should require enhanced

behavioral safety credentialing for that system — reflecting the systemic risk that a behavioral safety failure in a concentrated vendor would pose to the credit union system.

6. Coordinate with NIST and Peer Regulators

The NCUA should coordinate with the NIST AI Agent Standards Initiative and with peer regulators (OCC, FDIC, Federal Reserve) to ensure that behavioral safety credentialing standards for AI systems in stablecoin operations are consistent across the federal banking agencies. Credit unions should not face a different AI governance standard than national banks for functionally identical stablecoin activities. Interoperability of credentialing frameworks benefits credit unions by ensuring that vendors serving multiple types of institutions can obtain a single credential recognized by all regulators.

VI. The Cooperative Advantage

Credit unions have a structural advantage in AI governance that the NCUA should leverage: the cooperative model.

Credit unions are owned by their members. Their boards are elected by their members. Their mission is to serve their members' financial interests. This governance structure creates a natural alignment between the credit union's institutional interests and its members' interests in AI behavioral safety — an alignment that is less automatic in shareholder-owned banks where AI efficiency gains may be prioritized over AI safety investments.

The NCUA can leverage this alignment by framing AI behavioral safety credentialing not as a regulatory burden but as a member protection measure consistent with the cooperative charter. Credit unions that require their vendors to obtain behavioral safety credentials are protecting their members from discriminatory AI outcomes, from uninsured operational risk, and from the erosion of trust that AI behavioral failures would cause.

The credit union movement has a long history of collective action through CUSOs, leagues, and trade associations. Behavioral safety credentialing is well suited to this collective model: credit union trade associations (CUNA, NAFCU, state leagues) can negotiate group credentialing arrangements with vendors, reducing per-credit-union costs and ensuring consistent standards across the system.

VII. Responses to Specific NCUA Questions

We recognize that this proposed rule focuses on the licensing and application mechanics for stablecoin subsidiaries, with substantive prudential standards to follow in a subsequent rulemaking. Our responses to the NCUA's specific questions are framed accordingly — addressing what the application process and forthcoming Payment Stablecoin Issuer Manual should require regarding AI governance.

Question 5 (Challenges and Benefits of Application Requirements; Manual Structure): The most significant operational challenge credit unions will face in stablecoin activities is not the application process itself but the ongoing management of AI-driven compliance systems they cannot independently validate. The forthcoming Payment Stablecoin Issuer Manual should include a dedicated chapter on AI governance for stablecoin operations, covering: (a) minimum requirements for vendor AI governance documentation that applicants must obtain and submit; (b) behavioral

safety credentialing as an accepted form of AI governance evidence; (c) ongoing monitoring obligations for AI system performance, including behavioral drift and demographic impact; and (d) escalation procedures when vendor AI systems exhibit behavioral safety failures. The Manual should explicitly recognize that credit unions will rely on third-party vendors for AI compliance systems and should calibrate its guidance to the vendor-dependent operating model rather than assuming internal AI development capability.

Question 6 (Audited Financial Statements): We support the requirement for audited financial statements as part of the initial application. We further recommend that the NCUA extend the audit concept to the AI systems that stablecoin subsidiaries will deploy. Specifically, the Manual should recommend — and subsequent rulemaking should require — that applicants submit evidence of independent behavioral safety evaluation of the AI systems intended for BSA/AML compliance, reserve management, and consumer disclosure functions. This AI audit is the operational risk equivalent of the financial audit: it provides independent assurance that the systems performing consequential compliance functions meet defined performance standards.

Question 7 (IT and Operational Risk Management Documentation): This question directly addresses the AI governance gap we have described. The NCUA asks what documentation should demonstrate rigorous IT risk management standards, specifically regarding (a) distributed ledger infrastructure, (b) technology systems reliability, and (c) operational readiness for fiat redemptions. We recommend a fourth category: (d) **AI system behavioral safety**. Applicants should be required to provide documentation regarding the behavioral safety characteristics of all AI systems that will perform compliance, monitoring, or decision-making functions in stablecoin operations. Acceptable documentation should include: behavioral safety credentials from qualified independent bodies; demographic impact audit results for AI systems performing BSA/AML functions; behavioral drift monitoring parameters and escalation procedures; and human override procedures for AI-generated compliance decisions. This documentation requirement ensures that the NCUA evaluates not just the blockchain infrastructure but also the AI infrastructure that will determine whether the subsidiary's compliance program functions as intended.

Question 8 (Consumer Disclosures at Application Stage): Front-loaded consumer disclosures should include information about the role of AI systems in the consumer's stablecoin experience. When AI systems process redemptions, generate account communications, or make decisions that affect a member's access to their funds, the member should know that an AI system is involved, what behavioral safety standards that system meets, and how to escalate to a human decision-maker. These disclosures should be required as part of the initial application to ensure that AI transparency is designed into the stablecoin subsidiary's operations from inception, not retrofitted after launch.

Question 9 (Additional Factors for Application Evaluation): The NCUA should formally add AI governance quality as an evaluation factor for stablecoin subsidiary applications. Specifically, the NCUA should assess: (a) whether the applicant's AI vendors maintain governance programs consistent with the Treasury FS AI RMF; (b) whether AI systems intended for BSA/AML, reserve management, and consumer functions have been evaluated by qualified independent bodies; (c) whether the applicant has contractual provisions requiring vendors to maintain behavioral safety credentials and to notify the credit union of credential revocations or material behavioral safety failures; and (d) whether the applicant's board has adopted policies for oversight of AI risk in stablecoin operations.

Regarding Assessment of Fees (§ 706.104): We support the NCUA's authority to assess fees against subsidiaries for examination costs. We recommend that the NCUA's fee schedule reflect

the cost of AI governance examination, which will require specialized expertise beyond traditional safety-and-soundness review. Third-party behavioral safety credentialing reduces this examination cost by providing examiners with standardized, verifiable evidence of AI governance quality — shifting the burden of technical evaluation from the NCUA's examination staff to independent credentialing bodies.

Regarding Conditional Approvals (§ 706.106): We support the NCUA's authority to attach operational conditions to application approvals. We recommend that, for applicants deploying AI systems in consequential compliance functions, the NCUA consider conditions requiring: (a) maintenance of current behavioral safety credentials for vendor AI systems; (b) annual demographic impact audits of BSA/AML AI systems; and (c) reporting of material AI behavioral safety incidents to the NCUA within defined timeframes.

VIII. Cross-Reference: Treasury Section 9 Report

The Treasury's Section 9 report, *"Innovative Technologies to Counter Illicit Finance Involving Digital Assets"* (March 2026), independently validates the concerns raised in this comment. Section 4 of the report identifies AI and machine learning as essential tools for BSA/AML compliance in the stablecoin ecosystem, while acknowledging that AI deployment introduces resource burdens for smaller financial institutions, consumer privacy risks, and cybersecurity vulnerabilities.

These concerns apply with particular force to credit unions. Third-party behavioral safety credentialing addresses all three: it reduces resource burdens by enabling credit unions to rely on independent evaluation rather than building internal capacity; it incorporates data provenance auditing; and it includes adversarial robustness testing.

Closing

The GENIUS Act creates an opportunity for credit unions to offer their members access to stablecoin services that enhance financial inclusion, reduce transaction costs, and expand the cooperative model into the digital asset economy. Realizing this opportunity requires that the AI systems powering stablecoin compliance operate safely, accurately, and without discriminatory bias.

Credit unions cannot build this assurance internally. They should not have to. Third-party behavioral safety credentialing provides a proportionate, cost-effective, and scalable mechanism that aligns with the cooperative model, fills the vendor examination gap, and gives NCUA examiners the tools they need to supervise AI risk in stablecoin operations.

Empty Set LLC is developing the credentialing infrastructure that will enable credit unions, regulators, and insurers to verify the behavioral safety of AI systems in financial services. We urge the NCUA to incorporate behavioral safety credentialing into the GENIUS Act regulations — providing credit unions with a practical pathway to AI governance that protects their members and their cooperative mission.

We appreciate the opportunity to comment and welcome further dialogue with the NCUA and its staff on these matters.

Respectfully submitted,

Brice Love Co-Founder, Empty Set LLC brice@emptysetllc.com