510 LaGuardia Pl, 5th Floor
New York, NY 10012
April 20, 2026

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 1E-216
Washington, DC 20219

Re: Aleo Network Foundation Comment on OCC Notice of Proposed Rulemaking, Implementing the GENIUS Act for the Issuance of Stablecoins, Docket ID OCC-2025-0372

Dear Chief Counsel's Office:

I. Introduction

The Aleo Network Foundation (the "Foundation") appreciates the opportunity to submit comments in response to the Office of the Comptroller of the Currency's (OCC) notice of proposed rulemaking implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Docket ID OCC-2025-0372. The Foundation is a 501(c)(4) corporation that provides grants and other ancillary support to builders and developers on the Aleo Network and the broader ecosystem, with a focus on applied cryptography and zero-knowledge proofs in the context of decentralized technologies. The Foundation's leadership team includes former personnel from U.S. Military Special Operations Forces, the U.S. intelligence community, financial regulators, and large technology and payments firms.

The Aleo Network ("Aleo") is the first Layer-1 blockchain with programmable privacy built into its infrastructure. Powered by zero-knowledge cryptography, Aleo combines privacy-preserving features with smart contract programmability, enabling private, programmable transactions on a public, permissionless blockchain. Launched in 2024 and originating from Zexe,[1] a peer-reviewed zero-knowledge smart contract project, Aleo has formal integrations with Circle and Paxos Labs for stablecoin privacy solutions. The Foundation also has established partnerships with Circle, the Global Dollar Network, Google Cloud, and Request Finance, among others. The Foundation submits these comments to address a structural privacy gap in the proposed rule and to respond directly to Questions 12, 118, 120, and 121 regarding data privacy and risk management standards.

[1] Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu, "Zexe: Enabling Decentralized Private Computation," Cryptology ePrint Archive, Report 2018/962 (2018), https://eprint.iacr.org/2018/962.pdf.

II. Blockchain Transparency and the Consumer Privacy Problem

Most payment stablecoins today operate on fully transparent public blockchains, where every transaction—including amounts, counterparties, and frequency—is permanently and publicly visible. This is architecturally distinct from traditional banking, where transaction data is held confidentially by regulated institutions and disclosed only pursuant to legal process or customer consent. The proposed rule establishes meaningful consumer protection standards for permitted payment stablecoin issuers, including requirements to safeguard nonpublic personal information (NPI) consistent with the Gramm-Leach-Bliley Act. However, it does not fully account for the architectural reality of most onchain transactions. Where a stablecoin issuer operates on a transparent public blockchain, customer transaction data is exposed not through any failure of the issuer's internal controls, but by the design of the underlying ledger itself. The proposed rule's consumer protection framework does not address this source of exposure.

III. Observations on Specific Proposed Provisions

A. Definition of "Publicly Available Information" (Proposed § 15.2)

Proposed § 15.2 defines "publicly available information" to explicitly include data from a distributed ledger. Because the NPI protections in proposed § 15.13(b)(4) exclude publicly available information, on-chain transaction data falls outside those protections by design—regardless of whether the issuer played any role in making it public. The OCC should clarify that this carve-out does not relieve issuers of responsibility for the privacy of customer transaction data where the issuer has the technical means to prevent that data from becoming publicly available in the first place. Issuers who deploy on transparent ledgers when privacy-preserving alternatives exist should not benefit from the publicly available information exception as a matter of course.

B. Information Security and NPI Protections (Proposed § 15.13(b))

The information security program required under proposed § 15.13(b) is structurally undermined when the underlying ledger makes transaction data public by default. Notably, § 15.13(b)(4) requires safeguards to ensure the security and confidentiality of records containing NPI — but that protection is effectively moot for transparent blockchain issuers because the publicly available information carve-out in § 15.2 means on-chain transaction data never qualifies as NPI in the first place. With respect to Question 12, *“Is the term ‘nonpublic personal information’ appropriately scoped? How could the term be further refined or clarified?”*, the Foundation submits that the term "nonpublic personal information" is not appropriately scoped for the stablecoin context. The publicly available information carve-out—which explicitly includes distributed ledger data—effectively excludes the most sensitive category of customer financial behavior that stablecoin issuers generate: a permanent, publicly searchable record of every payment a customer makes. This is an anomalous result that has no analog in traditional banking. The OCC should refine the NPI definition to clarify that on-chain transaction data generated in connection with a customer relationship does not lose its protected status solely because it appears on a public ledger, where the issuer had the technical means to prevent that

exposure. More broadly, the spirit of GLBA-derived consumer protection requires addressing the source of exposure, not merely its downstream consequences. Issuers who cannot or do not implement adequate technical controls should, at minimum, be required to disclose prominently to customers that their transaction data is publicly visible on-chain.

C. Risk Management and Tokenized Reserve Assets (Proposed § 15.13)

Blockchain transparency creates distinct operational risks that the proposed rule does not fully address. For institutional users, publicly observable payment flows represent a competitive intelligence vulnerability—counterparties, transaction volumes, and payment timing are visible to any market participant with access to a blockchain explorer. These risks are particularly acute for corporate treasury applications and institutional payments, which represent a significant portion of projected stablecoin usage. The same concern extends to tokenized reserve assets under § 15.11(b)(8): to the extent reserve assets are tokenized on a public ledger, an issuer's reserve management operations—including the timing and size of asset purchases and sales—become publicly observable, creating potential front-running and market manipulation risks. Both of these transparency-driven risks fall squarely within the operational and information security risk management framework of § 15.13, and the OCC should recognize that privacy-preserving technical controls—including for tokenized reserve operations—constitute a sound risk management practice under that provision.

IV. Response to Questions 118, 120, and 121: Recommended Additional Data Privacy Standards

Questions 118, 120, and 121 invite comment on whether the proposed rule adequately addresses technology-specific risks, consumer protection compliance standards, and data privacy requirements under § 15.13. The Foundation's answer across all three is that the proposed rule leaves a material gap, and we offer the following specific recommendations.

Transaction Confidentiality as an Affirmative Standard. The OCC should establish transaction confidentiality as an affirmative data privacy standard for permitted payment stablecoin issuers—not merely a best practice. Question 118 asks whether § 15.13(b) should expressly address risks relating to encryption and other technologies; transaction confidentiality is precisely such a risk, and the answer should be yes. Specifically, the OCC should require issuers to assess whether their chosen blockchain infrastructure exposes customer transaction data to the public and, where it does, to implement technical controls proportionate to that exposure. This assessment should be incorporated into the risk management framework required under § 15.13 and should be subject to examination. Issuers who cannot implement adequate technical controls should be required to make clear, prominent disclosures to customers about the public visibility of their transactions.

Clarification that Privacy-Preserving Architectures Satisfy Proposed Rule Requirements. Some issuers may be uncertain whether deploying on a privacy-preserving distributed ledger is compatible with the proposed rule's requirements—particularly regarding reserve identifiability under § 15.11(a)(1)(i) and audit, reporting, and examination obligations under § 15.14. The OCC

should affirmatively clarify that privacy-preserving distributed ledger architectures, including those that cryptographically shield transaction details while maintaining the verifiability of transaction validity, fully satisfy these requirements. Such clarification would remove a regulatory barrier to the adoption of more privacy-protective infrastructure and would encourage issuers to make architectural choices that better protect consumers.

Recognition of Selective Disclosure as Sufficient for Examination and Transparency. The OCC should clarify that selective disclosure mechanisms—where issuers or account holders can cryptographically reveal transaction data to specific parties such as regulators and auditors, without requiring full public exposure on the ledger—are sufficient to meet the OCC's examination and transparency requirements. This distinction is important: full public transparency of transaction data is not necessary for effective regulatory oversight. Regulators and auditors can be granted cryptographic access to transaction records on a targeted basis, achieving the same supervisory objectives without exposing customer financial behavior to the general public. Establishing this clarification in the final rule would give issuers the confidence to adopt privacy-preserving infrastructure without fear of examination-related non-compliance.

Future Guidance. The Foundation recommends that the OCC commit to issuing guidance specifically addressing data privacy standards for payment stablecoin issuers as the market matures. This guidance should address minimum technical standards for transaction confidentiality, disclosure requirements for issuers who operate on transparent ledgers, and standards for selective disclosure to regulators and auditors. Given the pace of technological development in this space, guidance rather than rigid rulemaking would allow the OCC to remain responsive to evolving best practices.

V. Zero-Knowledge Proof Technology as a Path Forward

Zero-knowledge proofs (ZKPs) are a cryptographic technique that allows one party to prove to another that a statement is true—such as that a transaction is valid and properly authorized—without revealing any information beyond that fact. Applied to blockchain infrastructure, ZKPs allow transactions to be verified by the network without exposing transaction amounts, counterparties, or other details to the public ledger. This is categorically different from simply encrypting data: ZKP-based systems provide mathematical guarantees that transaction validity can be confirmed without disclosure, while also enabling selective disclosure to authorized parties through cryptographic tools such as view keys.

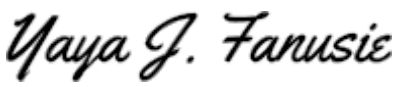
ZK-based privacy infrastructure is operationally available today and provides issuers a concrete, compliance-compatible path to meeting the standards recommended above. On a ZKP-enabled blockchain, an issuer can offer customers genuine transaction confidentiality while maintaining the ability to produce verifiable transaction records for regulators and auditors on request—without requiring full public exposure of that data. This architecture resolves the tension between consumer privacy and regulatory oversight that transparent blockchains create. The Aleo Network is an operational example of this infrastructure, and the Foundation invites the OCC to engage with us directly to better understand how ZKP-based systems function and how they can support the OCC's supervisory objectives.

VI. Conclusion

The proposed rule takes important steps toward establishing a sound consumer protection framework for payment stablecoin issuers. However, it does not account for the structural privacy problem created by transparent public blockchain infrastructure. The Foundation respectfully urges the OCC to: (1) establish transaction confidentiality as an affirmative data privacy standard under Part 15; (2) clarify that privacy-preserving distributed ledger architectures satisfy the proposed rule's operational, reserve, and consumer protection requirements; (3) recognize selective disclosure mechanisms as sufficient to meet examination and transparency requirements; and (4) commit to issuing further guidance on data privacy standards as the market develops. These steps would ensure that the consumer protection objectives of the GENIUS Act are met in practice, not merely in form.

The Foundation thanks the OCC for the opportunity to comment and looks forward to continued engagement on these issues.

Respectfully submitted,



Yaya J. Fanusie
Global Head of Policy
Aleo Network Foundation