

FinCEN/OFAC Stablecoin NPRM Comment Letter Summary and Implications for Zcash

Special Update | June 25, 2026

<https://community.pgpz.org/updates/20260625-Stablecoin-NPRM>

Not a PGPZ member?
Sign up here:



On April 10, 2026, the Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) released for public comment their joint Notice of Proposed Rulemaking (NPRM) implementing the GENIUS Act for Permitted Payment Stablecoin Issuers (PPSIs). The comment period closed on June 9, 2026.

Key Takeaways	Action Items
● Privacy technologies should not automatically trigger suspicious findings, especially since viewing keys allow examiners to verify compliance without exposing sensitive PII. ● Surveillance providers and others are pushing for incorporating requirements, including multi-source geolocation to block VPNs/Tor and mandatory tracking of all customer wallet addresses.	● Post/repost messaging that pushes regulators to decouple privacy-preserving features from assumptions of illicit intent. ● Push back against messaging that calls for blocking users who utilize VPNs, proxies or Tor routing.

Executive Summary

Although the proposed rule focuses on PPSIs and stablecoins, the regulatory mechanisms, compliance standards, and technological mandates discussed carry direct and indirect consequences for the Zcash ecosystem, its core infrastructure builders, and its users.

A deep-dive of the 78 comment letters available for review reveals a technically sophisticated debate regarding blockchain transparency. Multiple industry advocates, venture funds, and privacy-centric projects have actively discussed the viability of zero-knowledge cryptography, selective disclosure, and self-custody protections.

The majority of the comments demonstrate that the broader digital asset industry is shifting toward "data minimization" as a baseline security defense. Commenters explicitly warned that forcing institutions to link static PII to public blockchain ledger histories creates highly vulnerable corporate data honeypots. The comments suggest an industry consensus that ZKPs and decentralized, private identity credentials are functionally mature tools that regulators must accommodate under a technology-neutral framework. This provides a strong baseline for the Zcash ecosystem to position selective disclosure infrastructure as a gold standard for regulatory compliance.

Key Themes

The comment letters highlight six critical areas that may impact the Zcash ecosystem:

- **Absolute Protocol Autonomy vs. Intermediary Regulation:** Foundational legal and technical arguments are made, establishing that truly decentralized protocols cannot comply with Bank Secrecy Act (BSA) or sanctions monitoring frameworks because they lack legal entities, compliance officers, or centralized customer relationships. Commenters emphasized that regulations must focus exclusively on centralized financial intermediaries rather than automated, immutable protocol code layers.
- **Preserving the Cash Analogy and Token Fungibility:** Technical advocates compare secondary-market peer-to-peer crypto transfers to physical cash moving in open circulation, arguing that individual-to-individual asset movements should not independently trigger institutional reporting obligations. Furthermore, commenters warned that granting issuers sweeping, subjective discretion to block secondary-market transactions severely degrades token fungibility.
- **Defending Against Privacy Coin "Categorization" Bias:** Institutional operators (such as Circle) and technology investors (such as a16z) have forcefully argued that privacy-preserving technologies and privacy coin classifications must not automatically trigger Suspicious Activity Reports (SARs) or adverse regulatory findings absent behavioral indicators of explicit wrongdoing.
- **The Validation of Cryptographic Evidence and Viewing Keys:** A major subset of comment letters requests that federal agencies formally recognize tamper-evident, cryptographically generated records (viewing keys) as a valid method to discharge audit requirements. Commenters note that these frameworks allow examiners to independently verify protocol compliance without forcing the disclosure of sensitive personally identifiable information (PII) or internal screening logic—a direct validation of the structural utility of Zcash viewing keys.
- **The Identity Asymmetry ("A Sound Proof Can Certify a Ghost"):** Experts introduced a critical technical nuance regarding zero-knowledge proofs (ZKPs) and identity, noting that while ZKPs successfully verify that a specific on-chain credential is mathematically valid, they cannot inherently prove that the holder is a living, physically existing human principal.
- **Aggressive Network-Level Privacy Threats:** Surveillance and geolocation providers are lobbying for highly prescriptive rules that would require platforms to use multi-source geolocation to actively detect and block users utilizing VPNs, proxies, or Tor routing. Simultaneously, hawkish anti-corruption NGOs are calling for mandatory tracking of all direct customer wallet addresses and a total prohibition on interacting with addresses linked to mixers or privacy tools.

Actionable Recommendations for Zcash Stakeholders

Based on the NPRM and comments submitted, stakeholders within the Zcash ecosystem should consider execute the following strategic initiatives:

1. **Establish Legal Protections for Digital Bearer Instruments.** Defend protocol autonomy by leveraging legal precedents that frame shielded self-custody wallets as the direct digital equivalent of physical cash. Support compliance obligations that attach strictly to centralized financial intermediaries. This would help insulate open-source developers and automated, tamper-resistant protocol layers from traditional intermediary regulations.
2. **Demand Regulatory De-Biasing of Privacy Technologies.** Post/repost messaging that pushes regulators to decouple privacy-preserving features from assumptions of illicit intent. Policy frameworks must mandate that deploying on a privacy network, utilizing zero-knowledge proofs, or holding privacy-centric assets shall not categorically trigger Suspicious Activity Reports (SARs) or adverse risk findings absent independent, behavioral indicators of wrongdoing.
3. **Contest Overbroad Network-Level Surveillance Mandates.** Push back against messaging that calls for expanding regulatory proposals—such as requiring mandatory multi-source location triangulation, systematic address blacklisting, and the blocking of users utilizing VPNs, proxies, or Tor routing.

Summary of Comments

The table below summarizes the comments discussed in this memo.

Commenter / Organization	Relevant Topics/Issue Areas	Position Summary and Relevance to the Zcash Ecosystem
Blockchain Association	• Protocol Autonomy Limits • Smart-Contract Execution • Secondary Market Feasibility • Wallet-Level Freezing Limits	Argues that autonomous smart-contract execution does not constitute operational or transaction-level control by an issuer. Asserts that reaching into peer-to-peer secondary markets is legally flawed and technically infeasible due to the absence of a pre-settlement window. Notes that issuers are technically only capable of freezing entire wallets rather than individual assets. Recommends safe harbors modeled on the Digital Asset Market Clarity Act.
TRM Labs	• Decentralized Protocol Compliance • Data Minimization Principles • Freeze-Burn-Reissue Law • Intelligence Sharing Networks	Concludes that truly decentralized protocols mathematically and legally cannot comply with institutional mandates because they lack legal entities, compliance officers, or central operators; rules must target issuers, not code. Strongly advocates for "data minimization," warning that centralized databases of user financial data are vulnerable security targets. Notes that while technical capacity to reissue value exists, the legal standards are undefined. Highlights that this is the first time OFAC has codified an explicit sanctions compliance program requirement for a regulated asset class.
Midnight Foundation	• Privacy-Preserving Chains • Selective Disclosure / Viewing Keys • Cryptographic Outcomes • CDD Risk De-biasing	Argues that proposed compliance mandates erroneously assume a transparent-chain architecture. Asserts that selective disclosure using cryptographic viewing keys delivers equivalent or superior "regulatory visibility" compared to public ledger transparency. Demands that deploying on a privacy-preserving network must not itself be treated as an inherent CDD risk factor.

Commenter / Organization	Relevant Topics/Issue Areas	Position Summary and Relevance to the Zcash Ecosystem
Coin Center	• PII Overcollection and Honeypots • Public Ledger Identity Exposure • Zero-Knowledge Travel Rule • Intermediary Scoping	Warns that linking static personal identifiers to public blockchain addresses creates severe permanent surveillance exposure and security honeypots. Recommends that overcollection be officially recognized as a severe operational risk. Explicitly proposes a "zero-knowledge Travel Rule" leveraging attribute-based proofs and dynamic scoring to preserve consumer financial privacy.
Coinbax, Inc.	• Regulated Entity Attachment • The Cash Equivalent Principle • Functional Compliance Logic • Third-Party Operational Infrastructure	Advances the core principle that compliance obligations must attach to regulated financial institutions, not to individual transactions themselves. Explicitly analogizes peer-to-peer crypto transactions to physical cash moving in open circulation, stating that individual transfers do not independently trigger reporting obligations once an asset is issued. Pushes for flexible, outcome-focused engineering logic across centralized and decentralized architectures.
YEE! Technologies, LLC	• ZK Determinism vs. Physical Existence • "Ghost Certification" Risks • SAR Database Contamination • Agentic Transaction Records	Establishes a critical technical distinction regarding zero-knowledge proofs, stating that while on-chain mathematical determinism (ZKPs) successfully proves a credential's structural validity, it cannot verify the physical existence of a human holder, coining the paradigm: "a sound proof can certify a ghost." Warns that failure to utilize deterministic existence verification causes permanent contamination of FinCEN's database with non-existent subjects and AI-generated narrative drifts. Proposes verifiable records proving a human authorized agentic transactions.

Commenter / Organization	Relevant Topics/Issue Areas	Position Summary and Relevance to the Zcash Ecosystem
XSOC Corp.	• Pre-Transaction Cryptographic Controls • Post-Quantum Crypto Agility • Tamper-Evident Auditing records • Bounded Secondary Market Timeframes	Advocates for shifting from reactive post-transaction controls (wallet blacklisting) to proactive pre-transaction cryptographic authorization encoded directly into key-derivation paths ("Q-Sig"). Recommends a forward-looking mandate requiring an annually updated "crypto-agility roadmap" toward quantum-safe algorithms to prepare for evolving post-quantum environments. Joins another comment (Zhuravlev) in requesting that tamper-evident, cryptographically generated records be formally recognized as satisfying audit requirements without revealing underlying PII.
Circle Internet Group, Inc.	• Mixing Special Measures Withdrawal • Technology Category De-risking • Privacy Coin Exceptions	Urges FinCEN to withdraw its pending mixing special measures. Forcefully argues that broad technology categories—specifically naming privacy coins, mixers, and zero-knowledge proofs—must not be treated as categorically suspicious or automatically trigger SAR reporting mandates unless accompanied by independent, behavioral indicia of illicit activity.
Andreessen Horowitz (a16z)	• Mixing Rule Revision • Essential Lawful Anonymity • Indemnification Architectures	Demands that FinCEN rescind or heavily modify its pending mixing special measures. Argues that privacy-preserving technologies and zero-knowledge mechanisms are fundamentally essential for legitimate, lawful digital asset utility and must be legally insulated from broad regulatory overreach.
DDCP Foundation, Inc.	• Centralized Key Mandate Opposition • Self-Custody Wallet Protection • Digital Bearer Instrument Definition • Protocol Freezing "Blast Radius"	Opposes any regulatory framework that compels protocols to integrate a "centralized administrative key" into codebases. Frames self-custody wallets as cash-like digital bearer instruments. Cites recent enforcement temporary restraining orders to prove that centralized keys generate a destructive, overbroad compliance "blast radius" that disproportionately damages innocent secondary-market participants, urging decentralized co-signature alternatives instead.
GeoComply Solutions Inc.	• Multi-Source Geolocation Mandates	Demands prescriptive regulatory language forcing platforms to implement multi-source geolocation (GPS, cellular, Wi-Fi signal

Commenter / Organization	Relevant Topics/Issue Areas	Position Summary and Relevance to the Zcash Ecosystem
	• Anti-VPN / Proxy Controls • Enforcement Coding Requirements • Tor CircumventionBlocking	triangulation) to counter and block network-level privacy routing. Specifically targets the systematic tracking and circumvention of users utilizing VPNs, proxies, and Tor network routing. This represents a direct, systemic threat to network-level privacy infrastructure.
Transparency International U.S.)	• Mandatory Wallet Address Tracking • Systematic Mixer Blacklisting • Drop SAR Threshold to \$2,000 • Full Lifecycle Monitoring Mandates	Advocates for a highly hawkish, prescriptive framework. Demands a legal mandate requiring platforms to collect and verify all direct user wallet addresses, while systematically blacklisting any wallet interacting with mixers or privacy tools. Objects to the proposed \$5,000 SAR threshold, demanding it be dropped to \$2,000 for high-risk or secondary-market activity to capture micro-volume transfers.
Mona Armande	• Burn-and-Reissue Pathways • Official Government Custody Wallets • Foreign Issuer Enforcement Reach	Dedication to proving that "freeze-only is an incomplete compliance pathway" for asset recovery. Complying with a lawful order must explicitly encompass burning on-chain value and reissuing clean equivalent tokens directly into official government custody, court registries, or receiver accounts. Insists that foreign issuers serving U.S. persons must be strictly bound to comply with these orders via dependent U.S. banking architecture.
The Digital Chamber	• Verifiable Decentralized Identity • Zero-Knowledge Proof Integration • On-Chain PII Prohibition • DeFi Pricing Liquidation Protection	Strongly advocates for reusable, verifiable identity credentials and ZKPs to maintain baseline security. Insists on a strict regulatory prohibition against placing any personal identity information directly onto public blockchain layers. Warns that overbroad secondary-market blocking can distort pricing mechanisms and trigger cascading liquidation failures across DeFi liquidity pools.