

June 5, 2026

Via Electronic Submission: https://www.regulations.gov

Regulatory and Strategic Affairs Division Financial Crimes Enforcement Network
P.O. Box 39, Vienna, VA 22183

Re: Docket No. FINCEN-2026-0100; RIN 1506-AB73 Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements

To Whom It May Concern:

The Midnight Foundation ("Midnight" or the "Foundation") respectfully submits this comment in response to the joint notice of proposed rulemaking ("NPRM" or "Proposed Rule") published by the Financial Crimes Enforcement Network ("FinCEN") and the Office of Foreign Assets Control ("OFAC") on April 10, 2026 (91 FR 18582), implementing anti-money laundering, countering the financing of terrorism ("AML/CFT"), and sanctions compliance program requirements for permitted payment stablecoin issuers ("PPSIs") under the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act"), Pub. L. 119-27, 139 Stat. 419 (2025) (codified at 12 U.S.C. §§5901–5916).

Midnight is an organization dedicated to advancing the development, adoption and real world impact of the Midnight network, the privacy enhancing blockchain project designed for confidential smart contracts. Midnight enables compliant decentralized applications leveraging zero-knowledge proof ("ZK proof") technology, designed, amongst other uses for institutional and government use cases requiring selective disclosure—the ability to shield transaction data from public view while maintaining full regulatory access through cryptographic mechanisms.

We support the Proposed Rule's objectives: protecting the U.S. financial system from illicit finance while encouraging innovation in payment stablecoins. We commend FinCEN's decision to adopt a risk-based, effectiveness-focused approach rather than prescribing specific technical architectures. However, we write to identify a significant gap in the Proposed Rule that, if left unaddressed, could inadvertently prohibit an entire category of privacy-preserving payment technologies—technologies that deliver **equivalent or superior** compliance outcomes compared to transparent-chain architectures.

No single provision of the NPRM explicitly bans privacy-preserving stablecoins, however, the proposed rules consistently describe compliance mechanisms that assume transparent-chain architecture, without ever acknowledging the effective alternatives. The risk is not a prohibition — it is rather an interpretive framework that makes compliance impossible to demonstrate

without public blockchain data. In practice, exchanges and other intermediaries may incorrectly treat privacy chains as higher-risk for the reasons discussed in this comment. The explicit inclusion of self-hosted wallet and person-to-person activity in "secondary market" descriptions also signals that non-custodial flows are within Treasury's compliance focus, which can indirectly pressure listing policies for privacy-enhancing assets.

We respectfully request that Treasury should preserve room for compliant privacy-enhancing technologies, especially where they improve security, selective disclosure, and auditability without exposing all user data. We are concerned that the NRPM's broad emphasis on block/freeze/reject capability, sanctions compliance, and "secondary market" activity could create downstream incentives for exchanges and issuers to over-screen or de-risk privacy tokens and privacy chains. We further respectfully request that Treasury acknowledge zero-knowledge proofs, selective disclosure, auditable credentials, federated analytics, and similar tools as valid ways to manage risk without exposing full transaction graphs.

I. The Proposed Rule Contains an Unstated Transparency Assumption

In the NPRM, FinCEN and OFAC reference blockchain analytics, public blockchain data, and observable on-chain activity as primary mechanisms through which PPSIs satisfy their compliance obligations. An example of this is found in Proposed 31 C.F.R. § 1033.210(b)(1)(iii) Conduct Ongoing Customer Due Diligence, p18601) [1]. OFAC's Virtual Currency Industry Guidance, incorporated by reference, also recommends the use of blockchain analytics tools to monitor secondary market activity.

These references assume a specific technical architecture: a publicly transparent ledger where all transaction data (sender, recipient, amount, balance) is visible to any observer. This describes the current state of major stablecoin deployments on Ethereum, Solana, Tron, and similar networks. But it does not describe the only technically feasible architecture for compliant stablecoin issuance.

The risk is this: If FinCEN and OFAC finalize a rule whose compliance mechanisms are defined by reference to transparent-chain capabilities—without acknowledging alternative technical architectures that achieve the same regulatory outcomes—the Proposed Rule will likely act to discourage the adoption of privacy-preserving payment stablecoins, regardless of their compliance capabilities. This outcome would be both unintended and counterproductive.

[1] PPSIs *may also need to consider* information more narrowly tailored to the stablecoin market, including both *information available from public blockchains* and relevant off-chain considerations. Notably, as stated above, FinCEN assesses that the majority of illicit activity involving stablecoins occurs on the secondary market.Although the proposed rule would not impose a standalone, independent obligation on a PPSI to monitor secondary market transactions, consideration of such activity may be appropriate in the PPSI's development and maintenance of a customer risk profile (*e.g., public blockchains may indicate that a digital assets exchange that is a PPSI customer is engaged in deposits or withdrawal activity of the PPSI's stablecoin with addresses attributed to illicit actors* (emphasis added).

II. Mandatory Public Transparency Creates the Risks It Purports to Solve

Ironically, the transparency assumption embedded in the current framework creates its own set of risks—risks that privacy-preserving architectures are specifically designed to mitigate:

- **Financial surveillance of lawful activity.** On a transparent blockchain, any observer can see every transaction associated with a wallet address: amounts paid, amounts received, balances held, and counterparty interactions. If a resident pays property taxes with a transparent stablecoin, their wallet address is permanently linked to a public record. Data brokers, fraudsters, and hostile actors can aggregate this information at scale.
- **Competitive intelligence exposure.** Enterprises considering stablecoin adoption for treasury management, payroll, or supply chain payments face the prospect of exposing commercially sensitive transaction patterns to competitors, analysts, and the public. This is fundamentally incompatible with the confidentiality expectations that underpin the existing financial system and serves as a significant barrier to institutional adoption.
- **Gramm-Leach-Bliley Act tension.** For state-chartered banks exploring tokenized deposits on blockchain infrastructure, public transaction visibility may conflict with financial privacy obligations under Title V of the Gramm-Leach-Bliley Act (15 U.S.C. §§6801 et seq.) (the "**GLBA**"). A rule that implicitly requires public-chain deployment places bank PPSIs in an untenable position between federal AML requirements and federal financial privacy law. The GLBA requires financial institutions to protect the security and confidentiality of consumers' nonpublic personal information and to provide notice regarding information-sharing practices. The NPRM's expectations around monitoring, recordkeeping, sanctions screening, and lawful-order compliance should not be read to require generalized collection, retention, or disclosure of customer data beyond what is necessary to satisfy applicable legal obligations.

  Where privacy-preserving technologies can achieve AML/CFT, sanctions, and fraud-prevention objectives through selective disclosure, limited retention, or other risk-based controls, we respectfully request that Treasury please confirm that such approaches remain permissible. A contrary reading could force regulated intermediaries to over-collect and over-share personal information, creating avoidable tension with GLBA's privacy and safeguard expectations.

- **Transparent-chain analytics are already being evaded.** The agencies' own evidence in this NPRM demonstrates that illicit actors actively circumvent transparent-chain monitoring. The Proposed Rule describes how operators of the sanctioned Garantex exchange moved operational wallets containing stablecoins to new addresses on a daily basis specifically to evade detection by blockchain analytics services (91 FR 18587). If the compliance framework relies on public observability that sophisticated bad actors can already defeat through wallet rotation and chain-hopping, it is providing weaker

enforcement than a system in which compliance is cryptographically enforced at the transaction level before settlement occurs.

- **National Security Risk of Transactional Exposure.** Publicly transparent chains allow foreign adversaries to map the financial flows of U.S. defense contractors, government personnel, and critical infrastructure operators. A rule that *mandates* this exposure via transparency defaults creates a systemic intelligence vulnerability. Selective disclosure protects U.S. economic interests from foreign state-sponsored 'big data' surveillance.

We urge FinCEN and OFAC to recognize that the policy objective is not ***public transparency***—it is ***regulatory visibility*****.** These are not the same thing. Regulatory visibility requires that authorized parties (the issuer, regulators, law enforcement with lawful orders) can access transaction data. Public transparency requires that *everyone* can see it. The former is sufficient for every compliance purpose articulated in the Proposed Rule. The latter is an unnecessary and harmful side effect of current technical defaults.

III. Selective Disclosure Satisfies Every Obligation in the Proposed Rule

Privacy-preserving blockchains using selective disclosure architectures are not “privacy coins” in the commonly understood sense. They are not designed to prevent regulatory access. They are designed to prevent *public* access while preserving—and in some respects enhancing—regulatory access. We respectfully submit that a selective disclosure architecture can satisfy every material obligation articulated in the Proposed Rule:

Proposed Rule Requirement	Transparent Chain	Selective Disclosure
AML/CFT Program (§1033.210)	Issuer monitors public chain data and uses blockchain analytics	Issuer-issued payment stablecoins can be architected so the issuer retains a compliance viewing capability over the stablecoin's transactions via viewing keys
SAR Filing (§1033.320)	Issuer identifies suspicious primary market activity via account monitoring and public chain signals	Issuer identifies suspicious primary market activity via same account monitoring; transaction data available to issuer is identical or richer
CDD / Customer Risk Profiles	Risk profiles informed by on-chain activity visible to public and issuer	Risk profiles informed by on-chain activity visible only to issuer; deeper information asymmetry advantage over illicit actors
Block/Freeze/Reject (§1033.240)	Smart contract blacklists specific wallet addresses	Smart contract enforces equivalent controls: rejects transactions failing compliance circuits; freezes balances via issuer-controlled mechanisms

Lawful Order Compliance (12 U.S.C. § 5901 et seq)	Issuer freezes/burns/seizes the payment stablecoin/token at specified addresses; law enforcement verifies via public block explorer	Issuer freezes/burns/seizes the payment stablecoin/token using same smart contract capabilities; provides cryptographically authenticated evidentiary package to law enforcement via viewing keys; tamper-evident
OFAC Sanctions 31 CFR Part 502	Blockchain analytics screens public transactions against SDN list post-settlement	The issuer's payment stablecoin/token contract can require every transfer to include a zero-knowledge proof that neither party appears in an issuer-maintained sanctions set, rejecting non-compliant transfers before settlement
Travel Rule (§1033.410)	Sender/recipient info transmitted between their financial institutions via off-chain channels	Identical: sender/recipient info transmitted between their financial institutions via off-chain channels, with optional ZK attestation of data integrity
Recordkeeping (§1033.410)	Records maintained by issuer from public and internal data	Records maintained by issuer from viewing key access; cryptographically timestamped and tamper-evident

On every dimension, selective disclosure provides compliance outcomes that are functionally equivalent to—and in several cases stronger than—those achievable on transparent chains. The critical insight is that **the issuer retains the same visibility regardless of whether the public does.**

IV. Provision-by-Provision Analysis of Risks to Privacy-Preserving Architectures

We identify eight specific provisions in the Proposed Rule that, individually or collectively, could be interpreted to exclude privacy-preserving stablecoins. For each, we describe the risk and propose a targeted clarification.

A. Proposed §1033.240 — Technical Capability to Block, Freeze, and Reject

This is the most consequential provision for privacy-preserving architectures. It requires PPSIs to maintain "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State law, rules, or regulations." The NPRM also defines 'secondary market' to include transfers that occur through a PPSI's smart contract, including self-hosted-wallet and person-to-person activity, which may create downstream compliance pressure on privacy-preserving systems..

On transparent chains, PPSIs accomplish this by blacklisting wallet addresses. On a shielded chain, the same wallet addresses are not publicly visible. **But this does not mean the PPSI**

lacks the technical capability to block sanctioned parties. The mechanism is different, but the outcome is identical or stronger:

- **ZK-based sanctions screening:** The issuer's payment stablecoin/token contract can require transactions to include a zero-knowledge proof that neither party is a sanctioned person, using a cryptographic commitment such as a Merkle root by reference to an updated sanctions dataset maintained by the compliance operator. Transactions failing to produce a valid proof are rejected by the smart contract before settlement. This is pre-settlement enforcement, which is architecturally stronger than the transparent-chain approach of identifying violations after they have been recorded on an immutable ledger.
- **Viewing key access:** The PPSI can retain cryptographic viewing keys that provide full visibility into transactions involving its smart contracts on demand. When a lawful order is presented, the issuer produces a complete, cryptographically authenticated transaction record—including sender, recipient, amount, and timestamp—to the requesting authority. Because the revealed data can be verified against the chain's immutable commitments, the record is tamper-evident and more authoritative than a screenshot of a block explorer.
- **Freeze and burn capabilities:** Shielded payment stablecoins on a selective disclosure blockchain can be frozen, seized, and burned using the same smart contract mechanisms available on transparent chains. The PPSI's administrative control over the payment stablecoin contract is independent of the privacy architecture. Circle's ability to freeze USDC on Ethereum derives from the token contract, not from Ethereum's transparency—the same capability can be implemented identically on a shielded ledger.

Proposed clarification: The final rule should state that the "technical capability to block, freeze, and reject" standard is satisfied by any mechanism that achieves the required compliance outcome, including cryptographic enforcement mechanisms, regardless of whether the underlying blockchain provides public transaction visibility.

B. Proposed 31 CFR Part 502 — OFAC Sanctions Compliance Program

The NPRM contemplates that PPSIs must have technical capability to block, freeze, and reject impermissible transactions, including activity in the secondary market that may occur through smart contracts. OFAC's virtual-currency sanctions guidance also supports use of blockchain analytics as one compliance tool, but the overall compliance framework does not depend solely on public transaction data.

On a selective disclosure chain, the issuer has equivalent or superior sanctions screening capability through ZK-based pre-settlement enforcement. The Proposed Rule itself favorably references "the effective use of artificial intelligence, federated learning, and other advanced monitoring tools" as a factor in enforcement assessments. ZK proofs are precisely such an advanced tool.

Proposed clarification: OFAC should confirm that an issuer-implemented mechanism requiring cryptographic proof of non-sanction status—where transactions failing the proof are rejected before settlement—constitutes an "effective sanctions compliance program" under Part 502.

C. Customer Due Diligence — "Blockchains on Which the PPSI's Stablecoins Are Deployed"

The Proposed Rule states that CDD "may need to factor in" the "blockchains on which [the PPSI's] stablecoins are deployed" as a component of customer risk profiling. This provision creates the risk that deploying a payment stablecoin on a privacy-preserving blockchain could itself be treated as a risk factor by examiners—on the theory that the PPSI has less public observability of secondary market activity.

This interpretation would be incorrect. A PPSI issuing on a selective disclosure chain has *at least equivalent* information available to it than a PPSI on a transparent chain, because the issuer's viewing key access provides a privileged data set that is not available to the general public, mixing services, or chain-hopping obfuscation techniques. On a transparent chain, the data the PPSI sees is the same data everyone sees—including illicit actors who can design their behavior to evade detection. On a selective disclosure chain, the PPSI sees data that others cannot, creating an information asymmetry that favors compliance.

Proposed clarification: The final rule should specify that a PPSI's choice of blockchain architecture does not, by itself, constitute a risk factor for CDD purposes, provided the PPSI demonstrates equivalent regulatory visibility through alternative technical mechanisms such as viewing keys.

D. Proposed §1033.320 — SAR Filing and the "Preliminary Determination" on Secondary Markets

FinCEN commendably chose not to require PPSIs to file SARs on secondary market transactions. However, the Proposed Rule characterizes this as a "preliminary determination" and notes that secondary market SARs "could net highly useful information, particularly where the transfers do not occur through BSA-regulated institutions." This language signals that FinCEN may expand SAR obligations to secondary market activity in the future.

If secondary market SAR obligations are eventually imposed, the compliance mechanism matters. On a transparent chain, a PPSI would monitor public blockchain data for suspicious patterns. On a selective disclosure chain, the PPSI would monitor issuer-visible data via viewing keys for the same patterns. The analytical capability is identical—but on the selective disclosure chain, the PPSI's data cannot be observed or surveilled by blockchain analytics firms that lack viewing key access. That is appropriate rather than deficient: it means the PPSI is the authoritative source of transaction information, consistent with the BSA's structure of placing compliance obligations on the financial institution, not on third-party observers. Critically,

regulators and law enforcement do not lose oversight: they can be granted viewing-key access to audit the issuer's monitoring and verify its SAR determinations against the underlying data.

Proposed clarification: If FinCEN expands SAR obligations to secondary market activity in future rulemaking, it should confirm that issuer-accessible transaction data (including data accessible via viewing keys) satisfies the monitoring standard, and that third-party public observability is not a prerequisite for SAR compliance.

E. Lawful Order Compliance — 12 U.S.C. §5901(16) and §5903(a)(6)(B)

The GENIUS Act requires PPSIs to have the "technological capability to comply" with lawful orders to "seize, freeze, burn, or prevent the transfer of payment stablecoins." The Proposed Rule implements that requirement by requiring PPSIs to maintain the technical capabilities necessary to comply with such orders..

On a transparent chain, law enforcement can independently verify compliance by querying a public block explorer. On a selective disclosure chain, verification requires the PPSI to provide viewing key data to law enforcement, who can then cryptographically verify the record's authenticity. This introduces an additional step in the enforcement workflow—but it is a step that produces *superior* evidentiary output. A cryptographically signed, tamper-evident transaction record with a verifiable chain of custody is stronger evidence than a public block explorer query, which can be manipulated through screenshot editing, is not authenticated, and has no chain-of-custody guarantees.

Proposed clarification: The final rule should confirm that compliance with lawful orders does not require independent public verifiability of blockchain state, and that a PPSI's provision of cryptographically authenticated records via viewing keys constitutes adequate compliance with the lawful order mandate.

F. Proposed §1033.410 — Travel Rule

The Travel Rule requires PPSIs to transmit sender/recipient information to other participating financial institutions for transfers of $3,000 or more. The Proposed Rule brings payment stablecoin issuers into the applicable BSA/AML framework.

Travel Rule compliance is generally effected through off-chain exchange of required counterparty information between the transmittor's and recipient's financial institutions; it does not require public on-chain transparency, although firms may use on-chain analytics as a supplementary compliance control. On a selective disclosure chain, the Travel Rule can be satisfied identically to how it is satisfied on a transparent chain: the originating financial institution transmits the required data to the beneficiary financial institution. The privacy architecture of the underlying ledger is irrelevant to this off-chain data transmission.

However, if future rulemaking introduces a requirement that on-chain data must be reconcilable with off-chain Travel Rule transmissions, this would create an implicit public-visibility dependency.

Proposed clarification: The final rule should confirm that Travel Rule compliance is evaluated based on the off-chain data transmission between participating institutions, and does not require on-chain public verifiability of the underlying transaction.

G. Preamble References to "Public Blockchains" and "Blockchain Analytics"

Footnote 30 in the NPRM, in defining a blockchain, repeatedly refers to a 'public ledger,' and repeatedly references blockchain analytics as a compliance tool. Although the preamble is not regulatory text, it provides interpretive context that examiners and enforcement attorneys may use when reading the final rule. If the preamble consistently assumes public transparency as the technical default, every ambiguous provision in the regulatory text may be interpreted through that lens.

Proposed clarification: The final rule should clarify that references to 'public blockchains,' 'blockchain analytics,' or 'on-chain information' describe the public verifiability of the ledger and do not require public visibility of transaction contents. Where these terms appear as compliance tools, it should use technology-neutral language—such as "blockchain-derived data accessible to the PPSI"—that does not presuppose a particular ledger architecture.

H. Substantial Similarity Framework — 91 FR 16844 (April 3, 2026)

Treasury's separate proposed rule on "substantial similarity" principles for state regulatory regimes states that Treasury "generally expects that States would cross-reference [BSA/AML/CFT and sanctions] requirements." If the federal framework is finalized with an implicit transparent-chain assumption, any state that accommodates privacy-preserving stablecoins could be deemed "not substantially similar"—foreclosing state-qualified issuers from deploying on selective disclosure chains even if the state legislature has affirmatively recognized such architectures.

Proposed clarification: Treasury's substantial-similarity framework should evaluate whether a state regime achieves compliance outcomes equivalent to the federal framework, rather than whether it mandates a particular blockchain architecture. A state framework that recognizes selective-disclosure systems, including viewing-key access or other privacy-preserving controls, should rather be evaluated on whether it satisfies BSA, AML, sanctions, supervisory, and enforcement objectives..

V. The Agencies' Own Effectiveness Framework Supports Technology Neutrality

The Proposed Rule emphasizes that AML/CFT programs should be evaluated on their *effectiveness* rather than mere technical compliance. FinCEN has stated it will not pursue enforcement absent significant or systemic" program failures, and will consider favorably the "effective use of artificial intelligence, federated learning, and other advanced monitoring tools."

Zero-knowledge proofs are precisely the kind of "advanced monitoring tool" this framework contemplates. They enable cryptographic enforcement of compliance rules before transactions settle rather than relying on after-the-fact detection. A PPSI deploying ZK-based sanctions screening is not merely monitoring; it is **preventing** non-compliant transactions from executing. Pre-settlement prevention is a higher standard of effectiveness than the post-settlement detection that transparent-chain monitoring provides.

Furthermore, the GENIUS Act contains an innovation mandate. Section 9 (12 U.S.C. § 5908) directs the Secretary of the Treasury to seek comment on and research innovative methods to detect illicit activity involving digital assets, and directs FinCEN both to evaluate those methods against enumerated statutory factors — which expressly include 'privacy risks associated with the information that is collected or reviewed' (§ 5908(b)(2)(D)) — and to issue guidance and notice-and-comment rulemaking implementing them (§ 5908(d)). Congress thus built privacy directly into the statutory standard for evaluating AML detection methods: a technology that improves detection (factor A) and effectiveness (factor G) while minimizing privacy risk (factor D) is precisely what Section 9 directs FinCEN to favor. INATBA's Privacy Working Group, in its December 2025 position paper on the GENIUS Act, specifically identified this provision as creating an opportunity to incorporate privacy-enhancing technologies such as zero-knowledge proofs into the compliance framework. We concur.

VI. Summary of Specific Requests

For the agencies' convenience, we summarize our eight proposed clarifications:

1. **Functional equivalency standard for §1033.240:** Define "technical capability" by compliance outcome, not blockchain architecture.
2. **OFAC 31 CFR Part 502 technology neutrality:** Confirm ZK-based pre-settlement enforcement constitutes an effective sanctions compliance program.
3. **CDD chain-selection neutrality:** Specify that blockchain architecture choice is not itself a risk factor where the PPSI demonstrates equivalent regulatory visibility.
4. **SAR future-proofing:** Confirm issuer-accessible data via viewing keys satisfies any future secondary market monitoring obligations.
5. **Lawful order verification:** Confirm cryptographically authenticated records via viewing keys satisfy lawful order compliance without requiring public verifiability.
6. **Travel Rule independence:** Confirm Travel Rule compliance is evaluated on off-chain data transmission, not on-chain public visibility.

7. **Technology-neutral preamble language:** Replace architecture-specific references with outcome-neutral terminology, and clarify that 'public ledger' denotes ledger *verifiability*, not public visibility of transaction *contents*.
8. **Substantial similarity architecture neutrality:** Confirm state regimes recognizing selective disclosure are not penalized in the substantial similarity assessment.

VII. Real-World Precedent

Selective disclosure stablecoin architectures are not theoretical. Monument Bank, a fully regulated UK financial institution, is currently working to tokenize £250 million in customer deposits as shielded tokens on the Midnight blockchain. Deposit balances and transaction histories are cryptographically private; regulatory access is maintained through viewing keys. The UK's Financial Conduct Authority has not required public blockchain transparency as a condition of this activity.

In the United States, the Texas Blockchain Council is actively working with the Texas State Senate Business and Commerce Committee on stablecoin legislation that contemplates privacy-preserving payment architectures.

An ecosystem partner of Midnight, building applications on the Midnight network has responded to government RFIs in the United States (State of Indiana blockchain ecosystem RFI) and at the federal level (National Institutes of Health cancer data registry RFI), demonstrating the applicability of selective disclosure architectures to sensitive government use cases.

VIII. Regulatory Impact Considerations

Executive Order 12866 and the Regulatory Flexibility Act requires agencies to consider the costs and benefits of proposed rules and to evaluate the impact on small entities and consider alternatives that minimize economic impact while achieving regulatory objectives. A final rule that effectively prohibits privacy-preserving payment stablecoins—without an explicit finding that the compliance risks they present cannot be mitigated through alternative technical mechanisms—would impose significant costs:

- **Innovation costs:** An entire category of compliant payment technology could be foreclosed in the U.S. market, driving development and deployment to foreign jurisdictions.
- **Adoption barriers:** Institutional users—including banks, enterprises, and government agencies—that require financial privacy may be unable to use payment stablecoins.
- **Consumer protection costs:** Millions of stablecoin users could have their financial activity permanently exposed on public ledgers with no alternative.

- **Compliance quality costs:** Implementation of the Proposed Rule may disincentivize or effectively sideline pre-settlement cryptographic enforcement in favor of post-settlement monitoring and intervention, even though the latter is generally a weaker control from a risk-prevention perspective..
- **Evasion arbitrage:** As the Proposed Rule's own evidence demonstrates (Garantex wallet rotation, 91 FR 18587), sophisticated illicit actors already evade transparent-chain analytics. Prohibiting cryptographic enforcement removes the strongest available compliance tool while preserving the weakest.

These costs are avoidable. The Foundation's proposed clarifications do not weaken any compliance requirement. They ensure that the final rule's standards are defined by *what the PPSI can do* rather than *what the public can see.*

IX. Conclusion

The Midnight Foundation supports the Proposed Rule's core objectives and commends the agencies' risk-based, effectiveness-focused approach. We ask only that the final rule make explicit what the Proposed Rule implies: that compliance is measured by outcomes, not by architectural choices.

Privacy-preserving stablecoins with selective disclosure are not an evasion of the compliance framework. They are an **advancement** of it. They deliver the regulatory visibility the government needs while providing the financial privacy that citizens, businesses, and institutions expect. The technology exists and should be encouraged. The compliance architecture is demonstrable. The only question is whether the final rule will accommodate it.

We respectfully urge FinCEN and OFAC to adopt the eight clarifications summarized in Section VI and detailed in Section IV, ensuring technology-neutral language in the final rule that preserves the door for privacy-preserving payment innovation in the United States.

We appreciate the opportunity to comment on this important rulemaking and your consideration of this request. If you have any questions or would appreciate any technical demonstrations, architectural documentation, or further information that may be useful to the agencies, please contact Dr Saj Khoshroo at saj.khoshroo@midnight.foundation.

Respectfully submitted,

Midnight Foundation

Appendix A: Provision-by-Provision Risk Matrix

The following matrix identifies each provision in the Proposed Rule that poses a risk to privacy-preserving stablecoin architectures, the nature of the risk, and the Foundation's proposed clarification.

Provision	Risk	How It Targets Privacy Chains	Proposed Fix
§1033.240 Block/Freeze/Reject	Architecture-specific interpretation of "technical capability"	If interpreted to require public wallet blacklisting, shielded chains fail the test even though ZK compliance circuits achieve the same outcome	Define standard by compliance outcome, not mechanism; explicitly include cryptographic enforcement
OFAC Sanctions 31 CFR Part 502	Guidance references assume public chain analytics	OFAC's Virtual Currency Industry Guidance recommends blockchain analytics; shielded chains cannot be screened by third-party analytics firms	Confirm ZK pre-settlement enforcement meets "effective program" standard
CDD — Chain Risk Factor	Blockchain choice treated as risk signal	Deploying on a privacy chain could itself trigger elevated risk classification by examiners, penalizing the architecture regardless of compliance capability	Confirm chain architecture is not itself a CDD risk factor where issuer demonstrates equivalent visibility
§1033.320 SAR Filing	"Preliminary determination" may expand	If secondary market SARs are later required, the assumption of public data availability would disadvantage PPSIs on shielded chains	Confirm issuer-accessible viewing key data satisfies any future monitoring obligations
Lawful Order (12 U.S.C. § 5901 et seq)	Enforcement workflow assumes public verification	Law enforcement expects to verify via public block explorer; shielded chains require issuer-provided viewing key data, changing the workflow	Confirm cryptographically authenticated records satisfy lawful order compliance without public verifiability
§1033.410 Travel Rule	Future on-chain reconciliation risk	If on-chain data must reconcile with off-chain Travel Rule data, a shielded ledger creates a visibility dependency	Confirm Travel Rule compliance evaluated on off-chain transmission, not on-chain visibility
Preamble Language	Interpretive bias toward transparent chains	References to "public" blockchains and digital ledgers create an interpretive default that examiners apply to all ambiguous provisions	Replace architecture-specific references with technology-neutral terminology

Substantial Similarity (91 FR 16844)	Federal assumption overrides state innovation	States recognizing selective disclosure could be deemed "not substantially similar" to a federal framework that assumes transparency	Confirm state regimes evaluated by compliance outcomes, not architectural mandates