BLOCKCHAIN ASSOCIATION

June 9, 2026

The Honorable Andrea Gacki, Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
Post Office Box 39
Vienna, VA 22183

Re: Comment on Financial Crimes Enforcement Network and Office of Foreign Assets Control Joint Notice of Proposed Rulemaking Regarding Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements

Dear Director Gacki:

Blockchain Association ("BA") submits this comment in response to the U.S. Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC") Joint Notice of Proposed Rulemaking ("Proposed Rule") soliciting public comment on the proposed Anti-Money Laundering/Countering the Financing of Terrorism ("AML/CFT") Program and Sanctions Compliance Program Requirements for Permitted Payment Stablecoin Issuers ("PPSIs"), 91 Fed. Reg. 18582 (Apr. 10, 2026).

BA is the leading nonprofit membership organization dedicated to promoting a pro-innovation, pro-consumer policy environment for the digital asset industry.[1] BA endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can pave the way for a more secure, competitive, and consumer-friendly digital marketplace. BA represents more than 100 member companies that span a wide range of products that utilize blockchain and decentralized technologies, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem. Many BA member companies are building, supporting, or are deeply interested in stablecoin products in the United States.

[1] *See* Blockchain Association, https://theblockchainassociation.org.

I. Introduction and Executive Summary

BA supports FinCEN and OFAC's efforts to establish comprehensive AML/CFT and sanctions compliance requirements for PPSIs under the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act"). The misuse of stablecoins – or any digital asset – for illicit purposes should be aggressively prevented, and U.S. policy should reinforce strong safeguards against criminal exploitation of digital asset technologies. The digital asset industry stands ready to collaborate with FinCEN, OFAC, and other relevant authorities to strengthen safeguards, combat illicit finance, and ensure bad actors cannot exploit blockchain technology for unlawful purposes. The GENIUS Act reflects Congress's determination that payment stablecoin activity should be brought within a clear and workable federal regulatory framework that promotes responsible innovation while strengthening AML, CFT, and sanctions compliance obligations applicable to centralized issuers. The Proposed Rule appropriately recognizes that blockchain-based financial systems present distinct technological and operational considerations that differ materially from traditional intermediary-based financial systems. BA would like to highlight several effective aspects of the proposed rule, including:

- **Compliance in the primary market**: When addressing the use of blockchain technology in the Proposed Rule, FinCEN establishes a strong foundation to provide the necessary regulatory flexibility for peer-to-peer transactions in the secondary market. Correctly focusing compliance obligations on PPSIs in the primary market ensures that the Proposed Rule addresses risks presented by centralized issuers with meaningful customer relationships.
- **The freeze, seize, and block requirement:** The Proposed Rule states that PPSIs rightfully retain the technological capability and legal authority to seize, freeze, burn, or prevent the transfer of payment stablecoins in the primary and secondary markets pursuant to a lawful order. Further clarification of the term "lawful order" would provide PPSIs and enforcement officials with written guidelines for the legal process preceding the issuance of an order to seize, freeze, burn, or prevent the transfer of payment stablecoins.
- **The updated definition of Money Services Businesses ("MSBs")**: FinCEN's decision to carve out PPSIs from the MSB definition allows PPSIs to avoid duplicative reporting requirements and a registration regime that has historically been weaponized against developers of non-custodial, non-controlling blockchain technology.

While the Proposed Rule makes significant progress in adapting Bank Secrecy Act ("BSA") and sanctions compliance laws to the unique nature of blockchain technology, there are still some areas of the Proposed Rule that could be strengthened or clarified:

- **Results-based test**: The AML/CFT and sanctions compliance standards set forth in the Proposed Rule should be a results-based test that relies on overall adherence to the program rules, rather than a methodology-based test. This approach would provide PPSIs with flexibility to explore various solutions to combat illicit finance and satisfy the Proposed Rule's requirements, thus easing the compliance burden on PPSIs and encouraging the development of tailored solutions.
- **Narrow OFAC compliance obligations:** OFAC should align the final rule with the practical points at which PPSIs have direct customer relationships, usable counterparty information, and actual operational control – principally in issuance, redemption, reserve management, and fiat conversion. PPSIs do not intermediate peer-to-peer secondary market transfers, and autonomous smart contract execution should not be treated as indicative of transaction-level issuer control. The final rule should preserve FinCEN's secondary market Suspicious Activity Reports ("SARs") carve-out, affirm GENIUS Act requirements and OFAC's sanctions requirements are limited to primary market activity, and confirm that Specially Designated-Nationals ("SDN") address blocklisting, smart contract-level wallet freezing, and primary market sanctions screening satisfy PPSI obligations for secondary market sanctions risk.
- **Liability safe harbor**: FinCEN should adopt a liability safe harbor modeled on section 305 of the Digital Asset Market Clarity Act ("CLARITY Act") that protects PPSIs that act in good faith to temporarily restrict, freeze, seize, block, or prevent the transfer of payment stablecoins based on a reasonable belief of unlawful activity, a qualified written request from law enforcement, or a lawful order, while also clarifying that PPSIs are not required to act on isolated or unsubstantiated claims absent an independent legal obligation. Section 305 provides the right framework by protecting good-faith temporary holds, requiring reasonable procedural guardrails, preserving lawful freeze or seizure authority, and stating that covered persons are not compelled to freeze, seize, or block digital assets unless otherwise required under existing federal or state law.
- **Single registration requirement**: As PPSIs begin migrating from the MSB regime to the framework established under GENIUS, some PPSIs may find themselves without a clear regulatory path forward. PPSIs that offer other non-stablecoin digital assets will face dual registration requirements as both an MSB and a PPSI. FinCEN should clarify this complication in the final Rule and establish a single registration requirement for PPSIs that exchange other digital assets, thereby avoiding dual registration as both a PPSI and an MSB.

II. A Results-Based Approach to Compliance Would Prove More Effective and Efficient for Enforcement Officials, BSA Officers, and PPSIs

Blockchain technology is becoming increasingly integrated into the traditional financial system.[2] Everyday Americans' growing use of stablecoins reflects the utility of a dollar-pegged digital currency. The passage of the GENIUS Act, which established a practical regulatory framework for stablecoin issuers, was a crucial step toward onshoring issuers and positioning the United States as the global leader in digital assets. The current Administration has also prioritized "support[ing] growth and innovation in the digital assets industry, protect consumers, and keep the United States at the forefront of digital asset development."[3]

Like any transformative financial technology, stablecoins can be misused by illicit actors. The GENIUS Act addresses this reality by directing FinCEN and OFAC to establish requirements for PPSIs to maintain BSA and sanctions compliance programs, respectively. Therefore, it is imperative that FinCEN, OFAC, and other federal agencies protect American investors and businesses without stifling innovation or pushing liquidity offshore. To keep this industry onshore, BSA and sanctions compliance programs that FinCEN and OFAC implement must be results-based, and not capture technology that cannot comply with OFAC obligations. BA is encouraged to see FinCEN correctly focus its efforts on primary market activity.

Existing stablecoin issuers already utilize a variety of tools that would help satisfy the proposed AML/CFT programs and U.S. sanctions requirements, such as wallet address screening, suspicious wallet flagging, and real-time transaction monitoring.[4] Privacy-preserving compliance tools, including zero-knowledge proofs and cryptographic attestations, can enable PPSIs to demonstrate transaction compliance and sanctions screening to regulators without exposing underlying transaction data or counterparty identities. Furthermore, the BSA and sanctions compliance regimes of other centralized actors in the ecosystem, such as U.S.-based exchanges, custodians, and liquidity providers, complement PPSI compliance. These efforts, which exist throughout the ecosystem to reduce market manipulation, money laundering, and other illegal activities, include cybersecurity protections, KYC checkpoints when connecting a wallet to an intermediary, and tracing technologies that can track laundered funds directly to an individual

---

[2] Matthew L. Sigel et al., *State of Crypto 2025* (a16z crypto, 2025), https://dwt2zme5yrom6.cloudfront.net/uploads/2025/10/State-of-Crypto-2025-a16z-crypto.pdf.

[3] *Fact Sheet: The President's Working Group on Digital Asset Markets Releases Recommendations to Strengthen American Leadership in Digital Financial Technology*, The White House (July 30, 2025), https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-presidents-working-group-on-digital-asset-markets-releases-recommendations-to-strengthen-american-leadership-in-digital-financial-technology/.

[4] Chainalysis, *Stablecoin Risk Management*, https://www.chainalysis.com/stablecoin-risk-management/ (last visited June 9, 2026).

or criminal network.[5] The inherent transparency of blockchain networks, combined with modern compliance and tracing technologies, make digital asset rails a comparatively ineffective venue for money laundering, with illicit activity consistently representing less than 1% of total transaction volume.[6]

A results-based approach aligns with the GENIUS Act and the Proposed Rule's directive to treat PPSIs as financial institutions for BSA compliance. The framework established by the GENIUS Act, along with existing authorities codified in U.S. law, ensures that FinCEN, OFAC, and other federal regulators enforce these rules under the BSA and related statutes.[7] To ease this new compliance burden on PPSIs and encourage the use of emerging technologies, many of which are more effective than traditional means and based in the United States, enforcement officials should focus on whether an effective, well-maintained, risk-based AML/CFT and sanctions compliance program is in place by the implementation date.

A strictly methodology-based approach would limit innovation in compliance technologies, increase the cost burden on PPSIs to leverage "approved" methods, and restrict BSA officers from using potentially more effective means of combating illicit finance. Instead, a results-based assessment would enable PPSIs to explore and expand the compliance technology market, thereby strengthening competition and demand for the most effective methods to detect and deter bad actors. BSA officers and enforcement officials would spend less time evaluating a PPSI's individual compliance methodologies and instead focus on holistic program compliance.

III. Maintain the Proposed Rule's Focus on Primary Market Risks

FinCEN appropriately tailored the Proposed Rule to focus on primary market activity, where PPSIs maintain direct customer relationships and exercise meaningful operational control. Compliance obligations are effective when applied at centralized points of control, including issuance, redemption, reserve management, and fiat conversion, rather than dispersed across downstream secondary market activity where PPSIs lack meaningful customer information. FinCEN's proposed clarification in 31 C.F.R. § 1033.320(g) correctly recognizes this structural reality by providing that a secondary market transfer is not conducted "by, at, or through" a PPSI solely because the transfer interacts with the PPSI's smart contract. FinCEN also correctly concludes that imposing a blanket secondary market SAR obligation would require global

[5] Chainalysis, *Blockchain Security*, https://www.chainalysis.com/blog/blockchain-security/ (last visited June 9, 2026).
[6] Chainalysis, *2026 Crypto Crime Report*, at 3 (Mar. 17, 2026), https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-3-17-release.pdf.
[7] *See* Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act"), Pub. L. No. 119-27, § 9(d), 139 Stat. 419, 12 U.S.C. § 5901 *et seq.* (2025); 31 U.S.C. §§ 310, 5311, 5312(a)(2).

monitoring, produce reports containing little useful information, and incentivize defensive SAR filings with limited law enforcement value. The final rule should preserve that limitation and apply the same logic consistently across AML/CFT and sanctions obligations.

OFAC's proposed secondary market requirement, however, departs from that same logic. The proposed rule would require a PPSI sanctions compliance program to apply to all "payment stablecoin-related activity," and would require internal controls applicable to activity on the "primary or secondary market" that identify and "block or reject" activity that violates or would violate U.S. sanctions.[8] The proposed definition of "payment stablecoin-related activity" would sweep in issuing, trading, holding, transacting, transferring, redeeming, and other activity involving a PPSI-issued payment stablecoin from issuance until removal from circulation. OFAC further states that PPSIs should have technical capabilities, policies, and procedures to identify, block, and reject stablecoins traded by blocked persons in the secondary market when the PPSI exercises "possession or control" through smart contracts.[9] Similarly, FinCEN's proposed section 1033.240 would require PPSIs to have technical capabilities, policies, and procedures to "block, freeze, and reject" impermissible transactions, including transactions "by third parties" where the transaction results in an interaction with the PPSI's smart contract.[10]

That approach rests on an overbroad theory of issuer control. A PPSI does not intermediate, facilitate, approve, or participate in secondary market peer-to-peer transfers between third-party wallets. In a typical transfer, the sender's wallet signs and broadcasts the transaction to the blockchain network; distributed validators confirm and include the transaction in a block; and the transaction settles without the PPSI's involvement, approval, or knowledge. The PPSI's smart contract executes pre-programmed, non-discretionary code triggered by the transacting wallets. It does not identify the parties, conduct KYC, evaluate sanctions status in real time, or provide the issuer with a pre-settlement approval function.

That distinction is important. A bank or payment intermediary sits in the transaction flow and can decline to process a customer payment before settlement. A PPSI, once a payment stablecoin is circulating in secondary markets, generally does not occupy that position. Treating the mere execution of autonomous smart contract code as transaction-level issuer control would collapse the distinction between an asset issuer, an intermediary, and the execution of software code.

[8] Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, 91 Fed. Reg. 18,582, 18,660 (Apr. 10, 2026) (proposed 31 C.F.R. § 502.201(b)(3)(i)(B)).
[9] *Id.* at 18,660 (proposed 31 C.F.R. § 502.201(a), (b)(1)(i), (b)(3)(i)(A)–(B)).
[10] *Id.* at 18,665 (proposed 31 C.F.R. § 1033.240(a)).

Treasury's prior guidance supports a more disciplined control standard. OFAC's 2021 *Sanctions Compliance Guidance for the Virtual Currency Industry* states that, absent an exemption or authorization, U.S. persons must block property in their "possession or control" in which an SDN or blocked person has an interest.[11] In secondary market peer-to-peer transfers, the first condition is absent: the PPSI does not custody the stablecoins, hold the users' private keys, approve the transfer, reverse the transfer, or exercise discretionary transaction-level authority. A PPSI therefore should not be deemed to control a secondary market transfer solely because third-party wallets invoke its previously deployed smart contract.

FinCEN's 2019 Convertible Virtual Currencies ("CVC") guidance points in the same direction. FinCEN has recognized that a platform that merely provides a forum where buyers and sellers find each other, while the parties settle through outside wallets, does not qualify as a money transmitter.[12] FinCEN also recognized that a decentralized application developer is not a money transmitter merely for creating an application, even where the application facilitates CVC-denominated financial activity, unless the developer uses or deploys the application to engage in money transmission. Those principles are directly relevant here: deployment of code, standing alone, does not transform the deploying party into the intermediary for every later third-party transaction involving that code.

Further, the U.S. Court of Appeals for the Fifth Circuit's decision in *Van Loon v. Department of the Treasury* reinforces the same control principle. There, the court held that Tornado Cash's immutable smart contracts were not "property" of a foreign national or entity subject to OFAC blocking authority, emphasizing that the code was "unownable, uncontrollable, and unchangeable" even by its creators. The court further explained that, where a third party invokes an immutable smart contract, there is no operator on the other side of the transaction – there is "just software code" – and that Tornado Cash could not change, delete, remove, or otherwise control the immutable contracts.[13]

The proposed secondary market sanctions obligation is also technically infeasible under current blockchain architecture, where there is generally no meaningful pre-settlement window in which a PPSI can identify, review, and reject a peer-to-peer blockchain transfer before it settles; the PPSI does not sit in the payment flow; and attribution of wallet addresses to illicit actors often occurs after settlement. FinCEN's own SAR analysis confirms this reality.[14] FinCEN

[11] Office of Foreign Assets Control, U.S. Dep't of the Treasury, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 15, 2021), https://ofac.treasury.gov/media/913571/download?inline=.
[12] U.S. Dep't of the Treasury, Fin. Crimes Enf't Network, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, at 24, 27 (May 9, 2019).
[13] *Van Loon v. Dep't of the Treasury*, 122 F.4th 549 (5th Cir. 2024).
[14] *See* 91 Fed. Reg. 18,582, 18,607–08, 18,610 (Apr. 10, 2026) (discussing secondary-market SAR limitations and proposed 31 C.F.R. § 1033.320(g)).

recognizes that PPSIs may be unable to identify the actor behind a secondary market transaction, may have limited distinct insight into the parties or purpose of the transfer, and may generate low-value reports if required to monitor the entire secondary market.

The same smart contract interaction cannot simultaneously be too attenuated to support a secondary market SAR obligation and sufficiently robust to impose a real-time secondary market sanctions duty. FinCEN's proposed section 1033.320(g) correctly recognizes that a third-party transfer is not conducted through a PPSI merely because it interacts with a PPSI smart contract. OFAC's sanctions compliance framework should be aligned with that determination. Any other result would create regulatory inconsistency within the same joint rulemaking: the issuer would lack sufficient involvement to file meaningful SARs, while also being held responsible for maintaining the infeasible technical capabilities to identify and reject the transactions before settlement.

Nor does the GENIUS Act compel that result. The Act requires PPSIs to be treated as financial institutions for BSA purposes and to maintain technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions, as well as an effective sanctions compliance program.[15] Those requirements are properly read to apply where the PPSI has actual operational involvement: issuance, redemption, reserve management, minting, burning, customer onboarding, and other primary market activities. The Act cannot reasonably be read to impose sanctions compliance responsibility on PPSIs for the full universe of downstream secondary market transfers involving stablecoins already issued into circulation, particularly where the PPSI has no customer relationship, no contractual relationship, no custody, and no technical ability to intervene before settlement.

BA and its members respectfully recommend that FinCEN and OFAC:

1. Revise the definition of "payment stablecoin-related activity" to cover issuance, redemption, reserve management, and other activities in which a PPSI exercises direct operational involvement, and to exclude secondary market activity conducted solely by third parties.
2. Preserve proposed 31 C.F.R. § 1033.320(g), which appropriately recognizes that transactions are not conducted "by, at, or through" a PPSI solely because a secondary market transfer interacts with a smart contract.
3. Resolve the inconsistency between FinCEN's proposed secondary market SAR treatment and OFAC's proposed secondary market sanctions obligation by confirming that the

[15] *See* 12 U.S.C. § 5903(a)(5)(A), (A)(iv), (A)(vi) (treating PPSIs as financial institutions for BSA purposes and requiring "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions" and "an effective economic sanctions compliance program").

same smart contract interaction does not create transaction-level PPSI responsibility for either SAR filing or real-time sanctions rejection.

4. Confirm that a PPSI does not exercise "control" over peer-to-peer secondary market transactions solely because a smart contract self-executes autonomous code when invoked by third-party wallets.
5. Align the final rule's understanding of "control" with FinCEN's 2019 guidance and OFAC's 2021 virtual currency guidance, including the principle that control requires actual possession, custody, or discretionary operational authority over the relevant property or transaction.
6. Affirm that primary market actions involving the PPSI and its direct customers, including minting, redemption, and other PPSI-operated transactions, satisfy OFAC's "reject" capability requirement.
7. Confirm that maintaining up-to-date SDN wallet address blocklisting, smart contract-level freezing capabilities, and primary market reject controls satisfies a PPSI's sanctions obligations with respect to secondary market risk.
8. Establish a safe harbor for PPSIs that maintain current SDN List wallet-address blocklists, promptly implement official OFAC designations, take commercially reasonable remedial measures upon receiving attribution information, and cooperate with OFAC and law enforcement investigations.

IV. Uphold the Right for a PPSI to Seize, Freeze, Burn, or Prevent Certain Transactions Pursuant to a Lawful Order in Primary and Secondary Markets

BA supports FinCEN and OFAC's efforts to establish a clear and administrable framework governing when PPSIs may seize, freeze, burn, or prevent the transfer of a payment stablecoin pursuant to a lawful process. The ability of a PPSI to comply with valid legal process serves important law enforcement, national security, sanctions compliance, and consumer protection objectives, particularly where a PPSI maintains direct operational authority over issuance, redemption, or the underlying smart-contract functionality associated with a payment stablecoin.

The Proposed Rule appropriately recognizes that PPSIs may possess the technological capability to seize, freeze, burn, or prevent the transfer of payment stablecoins in both primary and secondary market contexts. These capabilities represent meaningful enforcement and risk-mitigation tools, particularly when combined with the transparency of public blockchain networks and the growing sophistication of blockchain analytics, transaction tracing, and investigative technologies available to both industry participants and law enforcement authorities. In practice, these capabilities have already enabled PPSIs and law enforcement

agencies to identify, freeze, recover, and reissue digital assets associated with fraud, sanctions evasion, cybercrime, terrorist financing, and other illicit activity.[16]

Nevertheless, the final Rule should more clearly distinguish between a PPSI's ability to comply with lawful process and any implication that PPSIs are required to maintain generalized surveillance obligations across all downstream secondary-market activity. The existence of technical capabilities to freeze, block, reject, burn, or seize payment stablecoins does not transform PPSIs into omniscient intermediaries with visibility into, or responsibility for, every downstream peer-to-peer transaction occurring on public blockchain infrastructure. Rather, these capabilities are appropriately understood as targeted enforcement tools that may be exercised with a proper final and valid lawful order.

Further clarification regarding the definition and scope of a "lawful order" would also improve legal certainty and administrability for both PPSIs and law enforcement authorities. In particular, the final Rule should clarify the degree of specificity required for lawful orders, including the wallet addresses for a PPSI to seize, freeze, burn, or prevent the transfer of assets. The final Rule should also clarify the meaning of "account" in the context of blockchain-based transactions, where traditional concepts associated with custodial account relationships may not readily apply.[17] Lawful orders should focus on the seizing and freezing of entire wallets, rather than individual assets or asset types within a single wallet. PPSIs are currently only capable of freezing or seizing entire wallets.

The final rule should also include liability safe harbor modeled on section 305 of the Digital Asset Market Clarity Act for PPSIs that, in good faith, restrict, delay, freeze, seize, burn, block, or prevent the transfer of payment stablecoins where the PPSI has a reasonable belief that the transaction, conversion, withdrawal, wallet, address, or account is connected to unlawful activity, or where the PPSI acts pursuant to a lawful order or a qualified written request from an appropriate government authority. Section 305 provides a workable framework: it protects a covered person that "voluntarily implements a temporary hold" in good faith from federal or

---

[16] Merkle Science, *How Blockchain Data Can Be Leveraged by Law Enforcement Agencies*, https://www.merklescience.com/how-blockchain-data-can-be-leveraged-by-law-enforcement-agencies (last visited June 9, 2026); TRM Labs, *Stablecoin Risk Management*, https://www.trmlabs.com/solutions/stablecoin-risk-management (last visited June 9, 2026).

[17] *See* FinCEN-OFAC NPRM (FINCEN-2026-0100), at 143:

> Question 29. Is FinCEN's proposed language specifying PPSIs must have the technical capabilities to block, freeze, and reject impermissible transactions occurring on the secondary market appropriately scoped and sufficiently clear? Does it capture activity it should not? Does it leave out activity it should include?
> Question 31. Should FinCEN refine or clarify the obligation related to having the technical capabilities to comply and actual compliance with the terms of lawful orders?
> Question 27. Should FinCEN refine or clarify the obligation related to having the technical capabilities to block, freeze, and reject impermissible transactions?

state private causes of action, including where the covered person acts based on a reasonable belief that the activity relates to an actual or attempted violation of federal or state law or after receiving a qualified written request from a covered agency.[18]

Section 305 also appropriately defines a qualified written request as a written communication from an authorized official of a federal or state law enforcement agency, including Treasury, that identifies a specific wallet, address, account, or transaction reasonably suspected of being linked to illicit activity, requests action with respect to that specified activity, and includes a designated agency contact.[19] FinCEN should incorporate similar procedural guardrails into the Proposed Rule, including reasonable time limits, customer-notice standards where appropriate, law-enforcement notification standards, and documentation requirements.[20]

FinCEN should also make clear that the rule does not compel or require a PPSI to freeze, seize, burn, block, or otherwise restrict payment stablecoins based solely on an isolated, unsubstantiated, or non-governmental claim where such action is not otherwise required under Federal or State law. That approach tracks section 305(c), which provides that nothing in section 305 may be construed to compel or require a covered person to freeze, seize, or block digital assets where such action is not otherwise required under existing federal or state law, while preserving lawful authority to seize or freeze assets pursuant to a lawful order or sanctions designation.[21]

FinCEN should clarify that a "lawful order" must, at a minimum, be a valid writ, process, order, rule, decree, command, or other requirement issued under federal law by a court of competent jurisdiction that requires a freeze or transfer restriction, identifies the payment stablecoins or accounts with reasonable particularity, and is subject to judicial or administrative review or appeal.[22] This balanced safe harbor would protect PPSIs that act proactively on credible evidence of unlawful activity, protect PPSIs that decline to act on unsubstantiated claims absent legal process, and provide law enforcement, issuers, and market participants with clear, uniform standards as payment stablecoin markets mature and scale.

Finally, the Proposed Rule's use of the terms "knowingly" and "actual knowledge" would benefit from additional clarification. The final Rule should expressly distinguish actual knowledge from constructive knowledge standards and clarify the circumstances under which a PPSI may be deemed to possess sufficient knowledge to trigger liability or affirmative compliance

[18] *See* Digital Asset Market Clarity Act, H.R. 3633, 119th Cong. § 305(b)(1), § 305(b)(1)(A).
[19] *See id.* § 305(a)(1), § 305(a)(4).
[20] *See id.* § 305(a)(5), § 305(b)(1)(B)–(C), § 305(b)(2).
[21] *See id.* § 305(c)(1), § 305(c)(3)(B).
[22] *See id.* § 305(e).

obligations.[23] Greater precision regarding the applicable scienter standard would improve administrability, reduce legal uncertainty, and support the implementation of appropriately risk-based compliance programs consistent with both the GENIUS Act and existing AML/CFT and sanctions frameworks.[24]

V. Retain and Clarify the Carve-out of PPSIs from the MSB Definition

BA supports FinCEN's proposal to exclude PPSIs from the definition of an MSB. The Proposed Rule appropriately recognizes that PPSIs should operate pursuant to the tailored statutory framework the GENIUS Act established, rather than through the duplicative application of the legacy MSB regime. This clarification is important given the historical uncertainty surrounding the application of the MSB framework to participants in decentralized blockchain ecosystems.[25]

The Proposed Rule would nevertheless benefit from additional clarification regarding PPSIs that engage in activities involving digital assets other than payment stablecoins. Specifically, FinCEN should clarify whether a PPSI remains subject to the MSB framework with respect to separate non-payment-stablecoin activities or whether PPSI status supersedes application of the MSB regime at the entity level. Absent such clarification, PPSIs could face overlapping registration, reporting, and supervisory obligations inconsistent with the GENIUS Act's objective of establishing a coherent and tailored federal framework for payment stablecoin issuers.[26]

VI. Conclusion

BA supports the Proposed Rule, which represents a meaningful and necessary step forward in strengthening the integrity of the U.S. financial system and establishing greater regulatory clarity in the digital assets industry. The provisions outlined in the Proposed Rule align with BA's longstanding commitment to robust compliance, transparency, and the responsible mitigation of illicit finance risks.

---

[23] *See* Intel Corp. Investment Policy Committee v. Sulyma, 589 U.S. 178 (2020).

[24] *See* FinCEN-OFAC NPRM (FINCEN-2026-0100) at 139 ("Question 6. Are there products or arrangements that may fall near the boundary of the proposed definition of payment stablecoin, and if so, how should FinCEN address such cases?").

[25] *See* U.S. Dep't of the Treasury, *Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash* (Aug. 23, 2023), https://home.treasury.gov/news/press-releases/jy1702; DeFi Education Fund, *Brief of Amicus Curiae DeFi Education Fund in Support of Plaintiffs-Appellees*, Van Loon v. Dep't of the Treasury, No. 23-50669 (5th Cir. Aug. 16, 2024), https://www.defieducationfund.org/uploads/pdf-imports/84ba66_063f9d1fd563466cadfa3f5434f918e9.pdf.

[26] *See* FinCEN-OFAC NPRM (FINCEN-2026-0100) at 138 ("Question 4. Should FinCEN carve PPSIs out of the MSB definition? Are there circumstances in which an entity could reasonably be uncertain whether it should be treated as a PPSI or as an MSB under the proposed definitions? If so, please describe.").

BA appreciates the significant effort and expertise that FinCEN and OFAC have dedicated to developing this regulatory framework and encourages FinCEN and OFAC to collaborate closely to harmonize their approaches. BA and its members welcome the opportunity to meet with FinCEN and OFAC officials at their earliest convenience to discuss the Proposed Rule and its implementation in greater detail.

Sincerely,

/s/ Ashok Pinto
Ashok Pinto
Executive Vice President
Legal and Government Relations