sifma Invested in America

sifma asset management group

June 9, 2026

BY ELECTRONIC SUBMISSION

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

Office of Foreign Assets Control
U.S. Department of the Treasury
Washington, DC 20220

RE: FinCEN and OFAC Joint Proposed Rulemaking on Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, Docket No. FINCEN-2026-0100, RIN 1506-AB73

To Whom It May Concern:

The Securities Industry and Financial Markets Association and its Asset Management Group (collectively, "SIFMA")[1] appreciate the opportunity to submit this letter in response to the joint notice of proposed rulemaking (the "NPR")[2] published by FinCEN and OFAC (together, the "Agencies") with respect to implementing provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (the

---

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation, and business policy, affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association.

SIFMA Asset Management Group ("AMG") brings the asset management community together to provide views on policy matters and to create industry best practices. SIFMA AMG's members represent U.S. and multinational asset management firms whose combined global assets under management exceed $45 trillion. The clients of SIFMA AMG member firms include, among others, tens of millions of individual investors, registered investment companies, endowments, public and private pension funds, UCITS and private funds such as hedge funds and private equity funds.

[2] Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC"), Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, 91 Fed. Reg. 18582 (Apr. 10, 2026).

"GENIUS Act" or the "Act")[3] pertaining to anti-money laundering/countering the financing of terrorism ("AML/CFT") program and sanctions compliance program obligations for permitted payment stablecoin issuers ("PPSIs").

SIFMA supports the development of a rigorous, practical, and risk-calibrated AML/CFT and sanctions compliance framework for PPSIs that protects the integrity of the U.S. financial system, promotes responsible innovation in payment stablecoin markets, and directs compliance resources toward the customers and activities that present the greatest illicit finance and sanctions risks. SIFMA's members expect to engage with payment stablecoins in multiple capacities, including as issuers, custodians, reserve asset managers, counterparties of PPSIs in short-term Treasury and repurchase markets, operators of institutional custody infrastructure, and providers of securities-related services in connection with stablecoin-related activities. SIFMA believes certain elements of the NPR should be clarified to ensure it is operationally workable and accounts for the distinct roles, operational capabilities, and risk profiles that PPSIs have in the payment stablecoin ecosystem.

In addition, because the U.S. legal and regulatory framework for digital assets and the underlying technology and markets are continuing to evolve, FinCEN and OFAC should commit to providing updated guidance and clarifications on a periodic basis to reflect legal, regulatory, and market changes. In particular, as legislation (under the Digital Asset Market Clarity Act ("CLARITY Act") or otherwise) and regulation further define the structure and regulation of U.S. digital asset markets, there are likely to be opportunities to further clarify and define the roles and interactions of PPSIs, digital asset service providers ("DASPs"), and other market participants.

I. Executive Summary

This letter addresses four topics:

- **Technical capabilities of PPSIs to block, freeze, and reject transactions in secondary markets:** The Agencies should provide clarity on when and how PPSIs are expected to block, freeze, reject, or otherwise prevent the transfer of payment stablecoins, particularly in the secondary market where a PPSI may lack a direct relationship with the transacting parties or sufficient visibility into relevant wallet holders, or in the absence of a lawful order, sanctions nexus, or other specific trigger for action. The final rule should preserve flexibility for PPSIs to use different technologies and controls; recognize infrastructural and practical limits based on the relevant ledger, smart contract, wallet architecture, and intermediary structures; and clarify how responsibilities should be allocated

[3] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, 139 Stat. 419 (2025).

where other payment stablecoin ecosystem participants, including DASPs, have greater user visibility. The Agencies should also confirm that blocking or freezing obligations apply to the relevant payment stablecoins or transaction, rather than to reserve assets. Absent such clarification, PPSIs may be subject to inconsistent or technically infeasible obligations, including where they lack sufficient visibility into transacting parties.

- **Safe harbor:** PPSIs should benefit from protections comparable to those available to other financial institutions when they take reasonable, good-faith actions to block, freeze, reject, delay, or otherwise restrict payment stablecoin transactions to comply with legal obligations or address suspected unlawful activity. The Department of the Treasury ("Treasury") should work with Congress to support enactment of legislation, such as proposed Section 305 of the CLARITY Act, to ensure that safe harbor protections cover the full range of actions PPSIs may take in good faith based on reasonably available information.

- **Scope of program requirements:** We support the risk-based approach to AML/CFT and sanctions compliance programs in the NPR, which is consistent with FinCEN's proposed AML program rule and should be applied consistently across financial institutions subject to AML/CFT program requirements. Our members would be concerned if the final rule's standards for PPSI AML/CFT programs, or its application in practice, departed from this risk-based approach or otherwise imposed heightened or bespoke obligations on PPSIs. In addition, because PPSIs will be regulated financial institutions subject to AML/CFT program obligations, they should be exempt from the definition of legal entity customer under FinCEN's customer due diligence rule.

- **Travel Rule:** The final rule should provide further guidance on Travel Rule obligations related to payment stablecoin activity and recognize reasonable, risk-based reliance on appropriately designed industry-developed solutions and standards as an acceptable means of compliance.

II. Recommendations

A. PPSI Obligations to Block, Freeze, and Reject Transactions on the Secondary Market Should Be Clarified

SIFMA recognizes that the GENIUS Act requires PPSIs to maintain "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations,"[4] and only permits PPSIs to issue payment stablecoins if they have "technological capability to comply, and

[4] 12 U.S.C. § 5903(a)(5)(A)(iv).

will comply, with the terms of any lawful order."[5] The NPR would apply these requirements to both primary and secondary market activity, covering transactions "by third parties, including where a transaction results in an interaction with a [PPSI's] smart contract."[6]

SIFMA appreciates the law enforcement utility of extending a PPSI's obligations to block, freeze, reject, seize, burn, or prevent the transfer of its payment stablecoins to the secondary market. We support the NPR's decision not to prescribe the specific technical capabilities, policies, and procedures that a PPSI may use to implement these requirements, in order to give PPSIs flexibility to use their own judgment about the best tools and approaches for their business and to "account for the development and implementation of new technology."[7] We also support the clarification that a PPSI would not be expected to "make an independent determination that a transaction violates federal or state law,"[8] and the decision not to extend suspicious activity monitoring and reporting obligations to the secondary market.[9]

The obligation to take certain actions with respect to secondary market transactions raises practical and technological issues, however, where further guidance would be helpful. We recommend the final rule address the following scenarios:

- The NPR indicates that obligations with respect to secondary market transactions will be "dictated by other federal or state laws, rules, or regulations, as well as

---

5 *Id*. at § 5903(a)(6)(B). A lawful order under the GENIUS Act "means any final and valid writ, process, order, rule, decree, command, or other requirement issued or promulgated under Federal law, issued by a court of competent jurisdiction or by an authorized Federal agency pursuant to its statutory authority, that—(A) requires a person to seize, freeze, burn, or prevent the transfer of payment stablecoins issued by the person; (B) specifies the payment stablecoins or accounts subject to blocking with reasonable particularity; and (C) is subject to judicial or administrative review or appeal as provided by law." *Id*. at § 5901(16).

6 NPR § 1033.240(a).

7 NPR, 91 Fed. Reg. at 18605.

8 *Id*.

9 *Id*. ("Notwithstanding the requirement to maintain technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations . . . this proposal would not require PPSIs to maintain separate internal policies, procedures, or controls as part of required AML/CFT programs to monitor secondary market activity independent of other obligations"). *See also id*. at 18607 ("FinCEN has preliminarily assessed that the burden of requiring PPSIs to file [suspicious activity reports] concerning secondary market activity would potentially outweigh the likely benefits.").

court orders," rather than through the independent determinations of PPSIs.[10] As a general matter, our members would not expect a PPSI to have sufficient information to make a blocking determination with respect to secondary market activity in the absence of a court order or an identified sanctions nexus, such as a sanctioned wallet address. If the Agencies have a different view or believe there are likely to be other sources of legal obligations upon which a PPSI should act independently, additional examples and clarifying guidance should be provided.[11]

- The specific actions a PPSI can take with respect to any particular payment stablecoin or payment stablecoin transaction may depend on the relevant ledger, smart contract, wallet architecture, or intermediary structure. For example, a PPSI may not be able to "reject" a blockchain transaction that has been made on-chain or return funds to the true originator where the sending address is an omnibus exchange wallet, a smart contract, or another intermediary-controlled address. In many such cases, freezing the relevant stablecoins or wallet may be the only feasible compliance response. In other cases, alternative technological methods, like burning and reissuing replacement coins, may achieve an equivalent result. The final rule should take a practical and flexible approach to evaluating whether a PPSI has established "the technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions."[12]

- In the secondary market, transfers may occur between persons with whom the PPSI has no direct relationship, and the PPSI's visibility into a transaction may depend on the design of the relevant smart contract.[13] The NPR acknowledges that, in many cases, other payment stablecoin ecosystem participants such as DASPs may have greater user visibility than PPSIs and may be better positioned to assess the legality of a transaction.[14] For example, a DASP may become aware

---

10 *Id*. at 18605.

11 SIFMA welcomes any guidance or resources that the Agencies may be able to provide to facilitate compliance. For example, OFAC should continue to publish sanctioned wallet addresses, including addresses that are known or suspected to be associated with sanctioned persons or territories.

12 NPR § 1033.240(a).

13 *See* NPR, 91 Fed. Reg. at 18607 (recognizing that "PPSIs may have less information on secondary market transactions than on primary market transactions. . . . At times, a PPSI could not identify an actor behind a secondary market transaction. PPSIs, like other financial institutions and law enforcement, can rely on the blockchain and analytical tools to gain greater insight into the risk associated with a particular transfer, but the PPSI may have limited distinct insight particularly as to the parties associated with, or the purpose of, the transfer.").

14 *See id*. ("[A]t times, secondary market transfers for which PPSIs have some visibility due to the smart contract may be subject to more ready observation by other [Bank Secrecy Act]-regulated institutions

of information linking a customer wallet to a sanctioned person or comprehensively sanctioned jurisdiction that is not available to the PPSI. In this circumstance, it would not be reasonable to expect the PPSI to freeze the stablecoins held by that wallet unless the DASP has communicated the relevant information to the PPSI. The final rule should make clear how responsibility to act with respect to secondary market transactions should be allocated between the PPSI and other intermediaries that may have more information about wallet holders.

- Cross-chain representations of payment stablecoins—where a payment stablecoin is represented on another blockchain through a third-party bridge, wrapped token, or other derivative token arrangement—raise distinct technical and compliance considerations. These derivative tokens effectively create a new financial product different from, but referencing, the payment stablecoin issued by the PPSI. Where created by a third party, the PPSI may have only limited or no control over the creation, redemption, or transfer of derivative tokens.[15] The final rule should provide guidance on how PPSIs should approach derivative tokens and other similar arrangements. In general, we believe the compliance responsibility to block, freeze, reject, burn, or otherwise restrict the derivative token should rest with the third party that issues the relevant derivative token or controls the relevant bridged asset infrastructure, rather than with the PPSI.[16]

- The final rule should also confirm that, consistent with current law, any obligation to block or freeze transactions applies only to the relevant payment stablecoins or payment stablecoin transaction, not to the underlying reserve assets held by the PPSI. Reserve assets are property of the issuer that supports its overall redemption obligations, and not the property of a specific payment stablecoin holder that may be subject to a block or freeze order.

---

or foreign financial institutions subject to reporting obligations. Such institutions may be better positioned to assess the suspiciousness of a transaction . . .").

[15] For example, "wrapped" payment stablecoins may be held in an omnibus or pooled account where individual stablecoins cannot be traced to the holders of the derivative tokens.

[16] Derivative tokens would appear not to qualify as payment stablecoins under the GENIUS Act because they are redeemable for another digital asset (the payment stablecoin) and, as such, their issuers would appear not to be regulated as PPSIs. *See* 12 U.S.C. § 5901(22) (defining "payment stablecoin" as a digital asset "the issuer of which (I) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value, *not including a digital asset denominated in a fixed amount of monetary value* . . .") (emphasis added). The Agencies should consider how issuers of derivative tokens based on the value of, and redeemable for, a payment stablecoin should themselves be regulated under the GENIUS Act and other relevant law, including with respect to their AML/CFT and sanctions compliance obligations.

B. PPSIs Should Have a Safe Harbor for Good-Faith Compliance Actions that Restrict Payment Stablecoin Transactions

The NPR would provide PPSIs the standard Bank Secrecy Act protection for suspicious activity report filings, including protection for voluntary reporting of possible violations of law or regulation.[17] That protection is important, but it does not address a distinct and increasingly significant issue for PPSIs: potential civil exposure for blocking, freezing, rejecting, delaying, or taking other compliance actions that restrict stablecoin holders' or counterparties' ability to transact.

In considering whether to take any such action, PPSIs will face time-sensitive decisions based on incomplete information. This will be particularly true in the secondary market, where alerts may be based on blockchain analytics, sanctions-screening hits, fraud indicators, law-enforcement information, or other risk signals that may favor rapid action before complete information is available. Without a specific safe harbor for good-faith actions, PPSIs may face private claims from holders or counterparties if a freeze, block, rejection, or similar compliance action is later determined to have been over-inclusive or otherwise mistaken.[18] That litigation risk could deter timely and appropriate compliance actions or encourage inconsistent responses across PPSIs.

PPSIs should receive protections comparable to those available to other financial institutions and market participants when they take good-faith action to comply with legal obligations or prevent potentially unlawful activity. Existing law already reflects this principle in related contexts, but it does not cover the full scope of compliance actions a PPSI might take with respect to its payment stablecoins. For example, under the International Emergency Economic Powers Act ("IEEPA"), compliance with any regulation, instruction, or direction issued under IEEPA provides full acquittance and discharge, and no person is liable in court "for anything done or omitted in good faith" in connection with the administration of, or pursuant to and in reliance on, IEEPA or a regulation, instruction, or direction issued under it.[19] The Anti-Money Laundering Act of 2020 similarly provides a safe harbor for financial institutions that keep an account or transaction open at the request of law enforcement, protecting such institutions from liability and adverse supervisory action solely for maintaining the account or transaction consistent with the request.[20] Section 305 of the CLARITY Act would protect covered

---

17 NPR § 1033.320(e).

18 Although PPSIs can take steps to establish contractual- or disclosure-based defenses to civil liability through, for example, appropriately drafted disclosures and contractually binding user terms and conditions, a safe harbor would be an important step to mitigate litigation risk.

19 50 U.S.C. § 1702(a)(3).

20 31 U.S.C. § 5333(a).

persons, including PPSIs, from federal or state private causes of action for good-faith "temporary holds"—restrictions that delay the execution of a transaction, conversion, or withdrawal involving digital assets for a reasonable period of time—implemented based on a reasonable belief that a transaction, conversion, or withdrawal relates to a violation or attempted violation of law or following receipt of a qualified written request.[21]

Treasury should work with Congress to support enactment of Section 305 or similar legislation to protect PPSIs from civil liability for reasonable, good-faith compliance actions taken as part of their obligations to maintain the technical capability to block, freeze, reject, or take similar actions with respect to the payment stablecoins they issue.

C. PPSI Program Requirements Should Follow the Risk-Based Approach that FinCEN Applies Consistently Across Financial Institutions

SIFMA supports the NPR's risk-based approach to AML/CFT and sanctions compliance programs for PPSIs. That approach is consistent with the broader direction of FinCEN's proposed AML/CFT program rule revisions, which emphasize that financial institutions should identify, evaluate, and mitigate their illicit finance risks through reasonably designed, risk-based programs and should allocate compliance resources in accordance with those risks.[22] The final rule should fully align with the framework FinCEN establishes when it finalizes its AML/CFT program rules and avoid imposing standards on PPSIs that would depart from the general risk-based approach applicable to other financial institutions subject to AML/CFT program requirements.

Prescriptive or one-size-fits-all requirements could divert compliance resources away from higher-risk activities and reduce the effectiveness of PPSI compliance programs. A risk-based framework instead allows PPSIs to tailor controls, monitoring, and resource allocation to the specific risks presented by their products, customers, counterparties, distribution models, and transaction activity.[23] Maintaining this approach would promote consistency across financial institutions, support more effective and

---

[21] Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Cong. § 305 (as ordered to be reported with an amendment by S. Comm. on Banking, Housing, and Urban Affairs, May 14, 2026).

[22] *See, e.g.*, FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism Programs, 91 Fed. Reg. 18704, 18710-11 (Apr. 10, 2026).

[23] We support the NPR's emphasis that AML/CFT programs should be risk-based and that more attention and resources should be directed toward higher-risk customers and activities rather than lower-risk customers and activities. NPR, 91 Fed. Reg. at 18597 & n. 170 (describing the factors considered when prescribing minimum AML/CFT program standards).

efficient identification and mitigation of illicit finance and sanctions risks, and allow compliance resources to be focused where they are most needed.

Because PPSIs will be regulated financial institutions subject to AML/CFT program obligations, FinCEN also should amend its customer due diligence rule to exempt regulated PPSIs from beneficial ownership identification and verification when onboarded by covered financial institutions, consistent with the treatment of other financial institutions regulated by a federal functional regulator or banks regulated by a state bank regulator.[24] An exemption for regulated PPSIs, when they are themselves customers of other covered financial institutions, would reduce duplicative onboarding obligations while preserving risk-based oversight.

D. Travel Rule Expectations Should Be Clarified and Should Permit Reasonable, Risk-Based Reliance on Industry-Developed Solutions

The NPR would require PPSIs to comply with the "Travel Rule," codified in 31 C.F.R. § 1010.410(f), and would amend the definition of "transmittal order" to expressly include payment stablecoins.[25] FinCEN states that it is not proposing to substantively change the relevant requirements other than to impose them clearly on PPSIs and clarify that transmittal orders involving payment stablecoins are covered.[26]

Compliance with the Travel Rule has raised practical and technological challenges across the digital asset industry, particularly where transfers involve wallet addresses, smart contracts, omnibus accounts, or intermediaries that do not map neatly onto traditional payment messaging frameworks. Market participants have worked to develop industry-led solutions for appropriately collecting and transmitting Travel Rule information in digital asset transactions. The final rule should acknowledge that reasonable, risk-based reliance on such industry-developed solutions and standards is an acceptable means of compliance, provided they are appropriately designed and implemented.

The final rule should also provide clarification regarding timing expectations for Travel Rule compliance, particularly where the relevant ledger or smart contract infrastructure cannot accommodate contemporaneous, on-chain delivery of the required information.

---

[24] *See* 31 C.F.R. § 1010.230(e)(2) (excluding from the definition of "legal entity customer" "[a] financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator").

[25] NPR, 91 Fed. Reg. at 18610. *See also* 31 C.F.R. § 1010.100(eee).

[26] NPR, 91 Fed. Reg. at 18610.

III. Conclusion

SIFMA appreciates the Agencies' consideration of these comments and supports the development of a robust AML/CFT and sanctions compliance framework for PPSIs. The targeted clarifications recommended above would strengthen compliance, promote consistent supervision, reduce unnecessary duplication, and better align responsibilities with the entities best positioned to identify and mitigate risk. SIFMA looks forward to further engagement with FinCEN, OFAC, and other regulators on the implementation of the GENIUS Act. Please contact Peter Ryan (pryan@sifma.org) or Bernard Canepa (bcanepa@sifma.org) if you wish to discuss the points raised in this letter further or have any questions.

Sincerely,

Peter J. Ryan

Peter J. Ryan, Ph.D.
Managing Director, Head of Digital Assets and International Prudential Policy
Securities Industry and Financial Markets Association

Bernard Canepa

Bernard Canepa
Managing Director,
Associate General Counsel
Securities Industry and Financial Markets Association