June 9, 2026

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

Re: RIN 1506-AB73: PPSI Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Requirements

To Whom It May Concern:

Paradigm Operations LP ("Paradigm") and Hyperliquid Policy Center ("HPC") appreciate the opportunity to comment on the notice of proposed rulemaking ("Proposed Rule") jointly issued by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC") regarding anti-money laundering, countering the financing of terrorism, and sanctions compliance requirements for permitted payment stablecoin issuers ("PPSIs") under the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act").

Paradigm is a frontier-technology investment firm that invests and builds in digital assets, AI, robotics, and across new technological frontiers from the earliest stages that has partnered with digital asset and blockchain companies building both decentralized ("DeFi") and centralized finance platforms.[1] HPC is an independent research and advocacy organization dedicated to advancing a clear, regulated path for Americans to access decentralized markets.[2] Hyperliquid is a general-purpose Layer 1 blockchain on which payment stablecoins are actively deployed and widely used as collateral, settlement, and trading assets across its onchain markets, including onchain perpetual derivatives markets.

We strongly support the GENIUS Act's core objective of fostering U.S. leadership across innovative blockchain technologies by establishing a regulatory framework for stablecoins that protects consumers, promotes U.S. government interests, combats financial crime and sanctions evasion, and ensures that U.S. developers will continue to drive the frontier of digital asset and blockchain innovation. In furtherance of those mutually shared goals, we submit the following comments focused on six specific aspects of the Proposed Rule, which we believe should be addressed in the final rule in order to meet the GENIUS Act's mandate:

[1] More information about Paradigm is available online at https://www.paradigm.xyz/.
[2] More information about HPC is available online at https://hyperliquidpolicy.org/.

- First, we urge FinCEN and OFAC to clarify PPSI and developer obligations related to trading activities in the secondary market.
- Second, we offer recommendations on the Proposed Rule's safe harbor provisions related to Suspicious Activity Report ("SAR") filings.
- Third, we request that FinCEN and OFAC clarify the Proposed Rule's obligations relating to blocking, freezing, or rejecting certain transactions.
- Fourth, we recommend a clarification regarding the scope of the Proposed Rule's requirements to comply with lawful orders.
- Fifth, we offer recommendations related to the Proposed Rule's Customer Due Diligence ("CDD") requirements.
- Finally, we offer comments related to OFAC's proposed obligations with respect to the secondary market and to OFAC's proposed elements of an effective sanctions compliance program ("SCP").

I. The Proposed Rule's Secondary Market Obligations

Paradigm and HPC welcome the Proposed Rule's distinction between primary and secondary market obligations of a PPSI. We agree that regulatory requirements for PPSIs should differ with respect to primary market activities, where PPSIs have a direct relationship with a customer, and with respect to secondary market activity, where they do not. The GENIUS Act repeatedly recognizes this distinction by, for example, requiring that PPSIs maintain "an effective customer identification program, including identification and verification of account holders *with the permitted payment stablecoin issuer*. . . ."[3]

This distinction makes clear that Congress intended that PPSIs should engage in due diligence on their own customers, while recognizing that PPSIs should not be required to do so for trading on the secondary market. Just as a bank is required to conduct KYC on its customers but not to monitor how those customers spend their cash once it is withdrawn, decentralized peer-to-peer transfers of stablecoins (and other digital assets) should require KYC only at the on- or off-ramps with regulated PPSIs. A contrary rule would require PPSIs to file an avalanche of noisy, false-positive-laden, low-value SARs that would create substantial costs for both PPSIs and FinCEN with little or no benefit to the U.S. government. As a result, Paradigm and HPC strongly endorse FinCEN's decision to refrain from requiring PPSIs to file SARs on secondary market activity and, with respect to Question 39, therefore urge FinCEN to not reconsider this approach.

Paradigm and HPC appreciate that FinCEN evaluated alternative, limited secondary market SAR reporting obligations, such as a requirement to file a SAR when a PPSI is notified about a suspected illicit transfer. However, we strongly agree with FinCEN's assessment that the burden of a reporting requirement in such circumstances would substantially outweigh any benefit the government might receive, particularly in light of the fact that PPSIs frequently have no access to non-public information about secondary transfers and the government's ability to obtain information using blockchain analytics, voluntary information sharing, and other modalities.[4]

[3] 12 U.S.C. § 5903(a)(5)(A)(v) (emphasis added).

[4] For this reason, and as discussed further below, we agree with FinCEN's proposal in §§ 1033.500, 1033.520, and 1033.540 of the Proposed Rule to apply the existing USA Patriot Act Section 314(b) framework, permitting PPSIs to share information about secondary market activity with the government and other regulated intermediaries. To the

Moreover, and for largely the same reasons, we also urge FinCEN to expressly confirm two additional points in its final rule. First, FinCEN should clarify that the "conducted through" safe harbor in § 1033.320(g) extends to downstream protocol developers and operators, including developers and operators of decentralized exchange protocols, lending protocols, and similar applications that have no direct relationship with the issuer. As currently drafted, § 1033.320(g) speaks to when a PPSI itself owes obligations but does not expressly resolve whether downstream developers and operators are independently covered, a gap that creates serious legal uncertainty for U.S.-based projects. Second, FinCEN should confirm that the Travel Rule does not apply to secondary market transfers in light of the fact that, as a technical matter, pseudonymous wallet-to-wallet transfers cannot carry the originator and beneficiary information the Travel Rule requires and a PPSI has no direct relationship with the parties to such transfers from which to collect that data. Expressly confirming these readings will provide both PPSIs and downstream protocol developers and operators the certainty they need when structuring their compliance systems.

II. The Proposed Rule's Reporting Safe Harbor

While Paradigm and HPC strongly endorse FinCEN's decision to not create a regulatory obligation for PPSIs to file SARs on secondary market activities, we see an opportunity for FinCEN to encourage better cooperation and information sharing between FinCEN and developers and operators of distributed ledger protocols, decentralized exchange protocols, and other software and platforms that serve persons who self-custody their digital assets by extending safe harbor provisions for voluntarily-filed SARs to these developers.

Since Congress first passed the Bank Secrecy Act ("BSA"), safe harbor provisions have encouraged financial institutions to report suspicious activities to FinCEN by shielding them from potential liability related to those reports, enabling critical cooperation between the government and the financial sector. Proposed § 1033.320(e)'s extension of these vital safe harbor provisions to PPSIs will ensure that they are able to share relevant information with the U.S. government without fear that they will inadvertently trigger criminal or civil legal liability for themselves.

But for exactly the same reasons, we also urge FinCEN and OFAC to expand the scope of the § 1033.320(e) safe harbor provisions to other downstream operators, including developers of distributed ledger protocols, decentralized exchange protocols, self-custody interfaces, and other platforms. While these developers will frequently have only limited information (for example, they typically may have no information other than a user's wallet address), they may want to share information with FinCEN and other U.S. government regulators about potentially suspicious or illicit transactions that they identify. Under the current Proposed Rule, however, these developers would not receive safe harbor protections should they choose to do so. Extending the safe harbor provisions to such developers would enable and strongly incentivize better cooperation between such developers and the U.S. government in combating illicit finance.[5]

---

extent suspicious patterns can be identified across the onchain ecosystem, the existing 314(b) framework provides the appropriate mechanism for PPSIs to share that information.

[5] To the extent that FinCEN and OFAC assess that they cannot expand the § 1033.320(e) safe harbor to non-PPSI developers, Paradigm and HPC urge FinCEN and OFAC to issue public enforcement guidance stating that they would

III. The Proposed Rule's Block, Freeze, and Reject Requirements

With respect to the Proposed Rule's obligation that PPSIs have the technical capabilities to block, freeze, and reject impermissible transactions, we welcome FinCEN's decision to refrain from mandating specific technical approaches and, instead, to allow PPSIs to develop and implement different approaches that will achieve more effective outcomes. While endorsing the decision to refrain from *requiring* any specific technological approach, however, we also recommend that FinCEN clarify that PPSIs that choose to adopt certain specific technological approaches *would* satisfy the technical capabilities requirements. This would provide PPSIs that choose to adopt certain industry-leading technological approaches regulatory certainty while also allowing further innovation.

Among the approaches that FinCEN and OFAC should deem sufficient to satisfy the block, freeze, and reject requirements are stablecoin architectures that impose transfer restrictions at the smart-contract level. These programmable control mechanisms can enforce compliance rules by automatically preventing transfers to specified addresses, applying transaction policies, and maintaining auditable records of permissioned actions. These controls operate programmatically and in real time, reducing the operational cost of compliance while ensuring that stablecoin activity remains within the regulatory perimeter established by the Proposed Rule. In many cases, these programmable control mechanisms will be more effective at achieving FinCEN and OFAC's AML/CTF objectives than other compliance approaches because they operate *ex ante*, rather than *ex post*, and cannot be circumvented by counterparty behavior.

Accordingly, the final rule should make clear that PPSIs issuing stablecoins on a distributed ledger protocol may rely on that protocol's inherent token controls as one method of fulfilling relevant compliance obligations under the GENIUS Act. Under this framework, PPSIs could still *choose* to adopt other approaches to meeting the technical capabilities requirement, but developers that seek regulatory certainty could obtain it by building to meet the specific technical requirements for the regulatory safe harbor.

IV. The Proposed Rule's Lawful Order Requirements

Paradigm and HPC recommend that FinCEN further clarify that the Proposed Rule's Section 5903(a)(6)(B) requirements related to the execution of lawful orders apply *only to PPSIs*, and not to developers, protocol contributors, or onchain network participants that bear no independent PPSI obligations. When Congress passed the GENIUS Act, it drew a deliberate line between "digital asset service providers," which include companies that issue, exchange, and custody digital assets as intermediaries, and the developers of software and platforms that individuals use on a self-directed, disintermediated basis, but which themselves do not issue, transfer, or custody digital assets.[6] Clarifying that the Proposed Rule's lawful order requirements apply only to PPSIs is consistent with that statutory distinction.

---

not take enforcement actions, such as sanctions enforcement action, against such developers who in good faith share such information with government agencies.

[6] *See* 12 U.S.C. § 5901(7)(A)-(B) (providing that a "digital asset service provider" *does not include* "(i) a distributed ledger protocol; (ii) developing, operating, or engaging in the business of developing distributed ledger protocols or

The Proposed Rule defines "lawful order" in § 1010.100(rrr) by incorporating the GENIUS Act's definition of "person," which is how the rule scopes who bears the obligation to develop technological capabilities to execute lawful orders under Section 5903(a)(6)(B). As drafted, however, proposed § 1010.100(rrr) could potentially be read to include developers of distributed ledger protocols, self-custodial software interfaces, and other technologies that Congress *excluded* from the GENIUS Act's definition of "digital asset service provider" *within* the lawful order requirement. This was clearly not Congress's intent, and we assume it is also not the intent of the Proposed Rule. Paradigm and HPC, however, recommend further clarifying this matter in the final rule by explicitly stating that the entities and technologies described in 12 U.S.C. § 5901(7)(B) are not included in the scope of the lawful order requirements.

Failing to issue this clarification would risk imposing a lawful order obligation on every Ethereum, Hyperliquid, Solana, and Layer 2 validator who validates a transaction involving a PPSI-issued stablecoin. The predictable result would be that U.S. validator stakes migrate offshore, U.S. block-building operations relocate, and the U.S. share of the chain validator base shrinks—outcomes contrary to both the GENIUS Act's onshoring objective and broader U.S. interests in the architecture of public blockchains.

V. The Proposed Rule's Customer Due Diligence Obligations

The Proposed Rule would require PPSIs, like other regulated financial institutions, to adopt risk-based procedures for ongoing CDD that enable the PPSI to understand the nature and purpose of customer relationships and to establish a baseline against which suspicious transactions can be assessed.[7] In connection with that proposal, we recommend that FinCEN and OFAC define "customer" and/or define the scope of a "customer relationship" to clarify that a wallet address that simply holds or transfers a stablecoin does not trigger CDD obligations, absent a direct relationship between the wallet owner and the PPSI.

Our recommendation is entirely consistent with how existing law applies to other financial institutions and with the text of the GENIUS Act. Regulations implementing the BSA currently define a "customer" as a person who opens an account, with an "account" being defined to include "a formal banking relationship established to provide or engage in services" and to exclude "[a] product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order."[8] The natural application of these definitions in the context of the GENIUS Act would cover cases in which a PPSI has a meaningful contractual relationship with a customer—such as direct issuance, custody, or provision of other services—and would not cover instances where a person simply uses a smart contract created by a PPSI (for example, where two self-hosted wallets trade a PPSI's token). However, in order to provide greater certainty, we recommend that FinCEN and OFAC explicitly confirm in the final

self-custodial software interfaces; (iii) an immutable and self-custodial software interface; (iv) developing, operating, or engaging in the business of validating transactions or operating a distributed ledger; or (v) participating in a liquidity pool or other similar mechanism for provisioning of liquidity for peer-to-peer transactions").

[7] 12 U.S.C. § 5903(a)(5)(A)(v).

[8] 31 C.F.R. § 1020.100(a)-(b).

rule that a wallet address that simply holds or transfers a PPSI-issued stablecoin does not constitute a "customer relationship" triggering CDD.

Our recommendation is also consistent with technical realities. PPSIs should and will generally have the technical capability to conduct CDD on customers with which a PPSI has a contractual relationship. But while a PPSI can see which wallet addresses hold its tokens and can observe transfers of those tokens on the blockchain to which the PPSI's token is deployed, a PPSI generally cannot obtain information about a wallet address, such as the address's ultimate owner, sufficient to enable the PPSI to engage in meaningful CDD.

And lastly, our recommendation is consistent with the decision Congress already made in the GENIUS Act to impose CDD obligations on "account holders *with the payment stablecoin issuer*,"[9] and not, for example, "persons transacting on the payment stablecoin's smart contract." Congress's choice of language was clearly intended to impose the CDD obligations in instances where a PPSI has a contractual relationship with a customer and not simply any wallet engaging in transactions involving the PPSI's stablecoin.

Paradigm and HPC also recommend that the final rule expressly recognize that programmable, smart-contract-based transfer restrictions and token-level blacklist controls—where implemented as an element of the PPSI's issued stablecoin—satisfy the issuer's obligations under Sections 5903(a)(5)(A)(iv) and (v) with respect to permissible holders and transferees. As discussed in Section III above, these mechanisms enforce compliance *ex ante* at the transaction layer, which is structurally a more effective approach to AML and sanctions compliance than traditional *post-hoc* monitoring, including for the government, by stopping unlawful transactions before they occur. Recognition of this architecture in the final rule would also satisfy the GENIUS Act's tailoring mandate at Section 5903(a)(5)(B) by enabling PPSIs to design compliance approaches that are tailored to their business models rather than requiring uniform layered-on compliance infrastructure.

VI. OFAC's Proposed Obligations and Enforcement Framework

Finally, Paradigm and HPC welcome OFAC and FinCEN's decision to codify the existing framework elements of an effective SCP. Beyond setting appropriate standards for PPSIs, codification of the existing five-element framework will provide PPSIs with greater certainty about the scope of GENIUS Act requirements and regulatory expectations by ensuring that a future administration cannot alter regulatory requirements without going through rulemaking processes and giving stakeholders an opportunity for input.

As a foundational matter, however, we urge OFAC to reconsider its position that simply deploying a smart contract constitutes the provision of a service to every person who interacts with that smart contract on the secondary market. Among other things, such a rule would mean that PPSIs may violate U.S. sanctions due simply to the fact that a blocked person used their smart contract on the secondary market, where the PPSI had no direct involvement in the transfer nor knowledge of the fact that a blocked person used the smart contract.

[9] 12 U.S.C. § 5903(a)(5)(A)(v) (emphasis added).

Paradigm and HPC understand the critical role that sanctions play in U.S. national security and why OFAC has historically taken a broad interpretation of the scope of U.S. sanctions obligations. Where persons are simply using a PPSI's smart contracts for trading on the secondary market, however, a PPSI does not function like a financial institution. Instead, it functions more like the developer of a telecommunications network, highway, or other piece of infrastructure on which others transact their business. A PPSI will often have no more knowledge of the identity of wallets transferring tokens using the PPSI's smart contract than a highway operator has of the identity of an individual riding in a car on the highway, and has a similarly negligible commercial relationship.

Practically speaking then, OFAC's interpretation and the implicit requirement that PPSIs must confirm the identities of wallets transacting on the secondary market is highly likely to create a chilling effect that will discourage PPSIs from deploying stablecoins to permissionless blockchains and instead only deploy stablecoins to permissioned ones. This chill will permeate the entire landscape, pulling U.S.-regulated stablecoins out of DeFi, undermine the GENIUS Act's intent to promote stablecoin innovation, and create a void filled by unregulated, off-shore, and non-dollar denominated alternatives. It would undo our current regulatory spring and restore the brutal winter of the past administration.

Moreover, OFAC's position is in tension with at least the U.S. Court of Appeals for the Fifth Circuit, which recently held that smart contracts were neither "property" nor "services" in the context of U.S. sanctions implemented pursuant to the International Emergency Economic Powers Act.[10] As a consequence of that finding, which the Treasury Department did not appeal to the Supreme Court, the Fifth Circuit held that OFAC could not lawfully sanction certain smart contracts. Treasury now seeks to effectively reverse the Fifth Circuit's holding by regulating third parties' use of certain smart contracts even where the smart contracts themselves are neither property nor services.

OFAC's position is also contrary to the approach that FinCEN is taking within the Proposed Rule, which, as discussed above, does not generally impose ongoing obligations with respect to the secondary market. It is difficult, if not impossible, to reconcile FinCEN's position in proposed § 1033.320(g) that a transaction "is not conducted or attempted by, at, or through a permitted payment stablecoin issuer only because a transfer by third parties results in an interaction with a permitted payment stablecoin issuer's smart contract" with OFAC's position that a PPSI's operation of a smart contract would provide a service to a blocked person trading on the secondary market.[11]

Accordingly**,** we urge OFAC to modify the definition of "payment stablecoin-related activity" in § 502.303 to exclude the mere development of a smart contract where a PPSI has no direct involvement in a transaction, does not receive a fee or other benefit related to the transaction, and

[10] *See Van Loon v. Department of the Treasury,* 122 F.4th 549 (5th Cir. 2024).

[11] Of course, 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," (including with respect to transactions that would violate sanctions laws). PPSIs should be able to meet this statutory requirement with respect to the secondary market by maintaining and enforcing a blacklist of identifiable addresses designated under OFAC sanctions programs, and blocking (or, in the case of a transaction involving an identified address from a sanctioned country that is not itself specifically blocked, rejecting) transactions involving such addresses.

is not otherwise directly involved in the transaction. Instead, OFAC should define "payment stablecoin-related activity" to include issuing, trading, holding, transacting, transferring, redeeming, or other activity involving a payment stablecoin issued by a PPSI from the time of issuance until the payment stablecoin's removal from circulation on the primary market, but not the secondary market.

Turning to the specific elements of OFAC's proposed codification of its compliance framework, we offer three specific recommendations:

First, we urge OFAC to further define an "effective" SCP. In particular, OFAC should afford a PPSI that has documented implementation of all five SCP elements, tailored to the PPSI's size and complexity and combined with periodic testing and auditing, a rebuttable presumption that its SCP is "effective" within the meaning of Section 5903(a)(5)(A)(vi). This presumption could be rebutted by evidence of material program failures, malice on the part of the PPSI, or other factors. But PPSIs that, in good faith, establish and maintain a SCP that meets the elements stipulated by OFAC should be entitled to rely on it as effective.

Second, we urge OFAC to specify reductions in civil penalties to which PPSIs would be entitled if they engage in an apparent violation of OFAC sanctions despite maintaining an effective SCP. OFAC's existing Enforcement Guidelines state that OFAC will consider "the existence, nature and adequacy" of an "OFAC compliance program" as one of several general factors that OFAC evaluates when determining its response to an apparent sanctions violation.[12] However, unlike several other agencies,[13] OFAC does not currently specify the specific reduction to which a company that maintains an effective SCP is entitled. Consistent with the practices of other agencies, we recommend that OFAC adopt and codify a reduction of up to 50% for any PPSI that maintains an effective SCP.

Third, we recommend that FinCEN and OFAC provide further clarity regarding what would constitute a "knowing" violation for a non-custodial PPSI, which is, among other things, a factor in determining the egregiousness and penalty amount of a purported compliance violation. Proposed Rule § 502.301 defines "knowingly" as a violation where "a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result," which is consistent with OFAC's definition of a "knowing" violation in other regulatory contexts. And as applied to traditional financial institutions, that standard works well: a bank can reasonably be expected to know its customers, know the nature of its transactions, and either identify sanctions issues or document why it failed to do so. With the relatively recent emergence of decentralized blockchains and OFAC's limited enforcement guidance to date, however, it is unclear under what circumstances OFAC would deem that a non-custodial PPSI "should have known" that it was engaging in a violation where the PPSI does not have a direct contractual relationship with a

[12] 31 C.F.R. Part 501 App. A III.E.

[13] For example, the Department of Justice's enforcement and voluntary self-disclosure policy that provides specific reductions in potential penalties for companies that meet certain requirements with respect to self-disclosure and other factors. *See* Department of Justice, 9-47.120 - Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, *available at* https://www.justice.gov/criminal/media/1400031/dl?inline. Similarly, criminal Sentencing Guidelines have long offered companies a reduction of up to three points in the formula for calculating penalties if a company maintains an effective compliance program. *See* U.S. Sentencing Commission Guidelines, § 8C2.5.

customer. We therefore recommend that the final rule provide greater clarity on this matter by specifying that where PPSIs do not have a direct relationship with a sanctioned entity and have implemented an effective SCP, they would be entitled to a rebuttable presumption that any purported violations were non-knowing.

* * * * *

Congress passed the GENIUS Act to establish a balanced legal framework that simultaneously provides regulatory certainty for stablecoin issuers, protection for stablecoin customers, and mechanisms to address money-laundering and financial crimes risk, while ensuring that American developers can continue to innovate. The comments in this letter are offered in that spirit, and we appreciate FinCEN and OFAC's consideration of the pro-consumer and pro-competitive benefits that they can unlock. If you have any questions or would like to discuss these comments further, please reach out to Stefan@paradigm.xyz or Brad@hyperliquidpolicy.org.

/s/ *Stefan Schropp*
Stefan Schropp
Senior Regulatory Counsel
Paradigm Operations LP

/s/ *Brad Bourque*
Brad Bourque
Policy Counsel
Hyperliquid Policy Center