VIA REGULATIONS.GOV

June 9, 2026

The Honorable Andrea Gacki
Director, Financial Crimes Enforcement Network
Attn: FINCEN-2026-0100
P.O. Box 39
Vienna, VA 22183

RE: Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, Docket No. FINCEN-2026-0100

Dear Director Gacki:

The Crypto Council for Innovation ("CCI") appreciates the opportunity to submit comments on the Notice of Proposed Rulemaking on Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements ("Proposed Rule" or "NPRM").

CCI is a global alliance of leading companies across the digital asset ecosystem, including stablecoin issuers, financial institutions, technology providers, and investors, with a mission to advance the responsible regulation of digital assets and demonstrate their transformational potential. CCI believes that achieving the shared goals of market integrity, consumer protection, and national security requires informed, evidence-based policy developed through constructive engagement with regulators. To that end, CCI respectfully offers the following comments and recommendations.

I. Summary

CCI supports Treasury's objective of establishing a clear and workable AML/CFT and sanctions compliance framework for permitted payment stablecoin issuers ("PPSIs"). A well-calibrated final rule will strengthen market integrity, reduce illicit finance risk, and provide the regulatory certainty the stablecoin industry needs to operate responsibly. The Proposed Rule reflects meaningful engagement with the GENIUS Act's directives and a genuine effort to calibrate obligations to the PPSI context. To that end, CCI supports Treasury's implementation effort and offers comments that will help FinCEN and OFAC clarify expectations for PPSIs, financial institutions supporting payment stablecoin transactions, and consumers.

CCI's comments address the following areas:

- The scope of PPSI obligations with respect to the secondary market, including the boundary between PPSI and money services business ("MSB") frameworks for issuers conducting activities beyond stablecoin issuance;
- The definition of "lawful order" and its application to wallet addresses;
- The technical capability requirements to block, freeze, and reject transactions — including the challenges posed by smart contract architecture and the absence of a safe harbor for good-faith blocking actions;
- Post-attribution sanctions liability: confirmation that PPSIs will not face retroactive exposure for transactions processed before a wallet was officially designated or flagged;
- Suspicious activity reporting obligations and their interaction with secondary market activity, including information sharing between affiliated entities;
- Currency Transaction Report ("CTR") filing responsibility when stablecoin activity occurs through ATM or kiosk operators;
- Sanctions compliance program implementation, including technical controls for secondary market transactions and the scienter standard applicable to the enhanced civil penalty tier; and
- Implementation timeline: a 12-month approach that completes the aims of the GENIUS Act.

CCI respectfully requests that FinCEN and OFAC consider the clarifications and recommendations set forth below in finalizing this rule.

II. CCI's Support for the Proposed Rule's Core Structure

Before turning to the areas where CCI seeks clarification or refinement, CCI seeks to affirm several aspects of the Proposed Rule that reflect sound regulatory judgment and should be preserved in the final rule.

Risk-Based Approach and Calibration to PPSI Complexity

CCI supports FinCEN's decision to ground the Proposed Rule in a risk-based framework that calibrates obligations to each PPSI's risk profile, size, and complexity. This approach encourages

effective, targeted compliance rather than uniform checkbox requirements that may be ill-suited to the range of business models that will operate under the PPSI framework.

The $5,000 SAR Threshold

CCI supports FinCEN's proposal to set the SAR filing threshold for PPSIs at $5,000, rather than the $2,000 threshold that currently applies to money services businesses. This calibration appropriately reflects the institutional nature of primary market PPSI activity and aligns PPSIs with other financial institution types subject to customer identification program requirements.

Innovation Credit in the Enforcement Framework

CCI affirms FinCEN's proposal under § 1033.221(d) to consider a PPSI's demonstrable efforts to advance AML/CFT priorities — including the use of innovative analytics and compliance tools — as a factor in enforcement and supervisory actions. This approach appropriately incentivizes investment in effective, forward-looking compliance infrastructure. CCI encourages FinCEN to issue guidance clarifying how it will assess and credit innovative compliance activities in practice, so that PPSIs can invest in novel tools with confidence that their efforts will be recognized. CCI also recommends that in addition to considering innovative tools, FinCEN consider a PPSI's innovative activities that support AML/CFT goals while mitigating de-risking, such as implementing programs to increase financial access for under-banked populations and improving remittance corridors in hard-to-reach geographic locations.

III. Secondary Market Obligations: Scope and Clarity

The Proposed Rule's treatment of secondary market activity is the most consequential structural question for PPSIs. FinCEN has drawn a careful line between primary market obligations — where PPSIs have direct customer relationships and clear visibility into transactions — and secondary market activity, where that visibility is limited. CCI supports this framework.

CCI also welcomes the limiting principle stated in the NPRM preamble: that the rule does not require PPSIs to maintain separate internal policies, procedures, or controls to monitor secondary market activity independent of other obligations. As it relates to the AML/CFT program requirements, this principle provides important clarity and CCI asks FinCEN to reaffirm it explicitly in the final rule. CCI notes, however, that the extent to which U.S. sanctions law independently creates secondary market obligations for PPSIs is a distinct question — one that turns on OFAC's authority rather than FinCEN's — and is addressed in Section V below. CCI's

endorsement of the limiting principle here should not be interpreted as taking a position on the scope of those separate sanctions obligations.

A. PPSI Carve-Out from the MSB Definition (RFC Question 4)

CCI supports a clear carve-out distinguishing PPSIs from money services businesses ("MSB"). Without it, entities transitioning from MSB to PPSI status risk operating under duplicative or conflicting compliance obligations during the transition period. CCI recommends that FinCEN issue guidance confirming how existing MSB compliance programs will be treated during that transition and providing clarity for any entity that may be uncertain whether it qualifies as a PPSI or an MSB under the proposed definitions.

CCI also asks FinCEN to clarify the scope of Part 1033 obligations relative to a PPSI's broader business activities. Where a stablecoin issuer also operates as an MSB— conducting activities beyond stablecoin issuance, such as exchange or transmission services — FinCEN should confirm that Part 1033 applies only to activities directly related to the PPSI's stablecoin issuance function, and that the applicable MSB framework continues to govern all other activities. The PPSI framework should be targeted and additive, not a wholesale displacement of existing MSB obligations for activities outside the issuance function.

B. Secondary Market Scope of the AML/CFT Program (RFC Question 8)

FinCEN's demarcation between primary and secondary market obligations is a necessary and welcome clarification. CCI asks FinCEN to go one step further and provide guidance on how on-chain data about secondary market activity can appropriately be incorporated into a PPSI's AML/CFT program design — for example, as an input to primary market customer risk assessments. CCI also asks FinCEN to clarify the boundary between the risk awareness that is expected and the active monitoring that is not required, so that PPSIs can design compliant and effective programs that are properly scoped.

C. SAR Obligations and Secondary Market Activity (RFC Question 35)

CCI supports FinCEN's preliminary decision not to impose SAR obligations for secondary market transactions. This should be codified in the final rule. PPSIs generally do not have any unique visibility into secondary market activity that differs from the same on-chain information that anyone can view via blockchain explorers and blockchain analytics. And without a direct customer relationship, any reporting obligation would likely produce low-quality filings, coming days or weeks after the transaction occurred, of limited value to law enforcement while imposing substantial operational burden.

CCI seeks clarification on one related point. The safe harbor under § 1033.320(e) protects PPSIs from civil liability for filing SARs and from liability for failing to notify persons identified in a SAR filing. CCI asks FinCEN to confirm that this protection applies equally to voluntary SAR filings

relating to secondary market activity, so that PPSIs are not deterred from making voluntary reports where they believe doing so would be useful.

CCI also asks FinCEN to confirm that the Part 1033 framework does not limit information sharing between a PPSI and its affiliated entities for compliance purposes. Where a PPSI operates as a subsidiary or affiliate of a larger financial institution, existing BSA guidance permits the sharing of SAR information and other compliance intelligence across the corporate family. FinCEN should confirm that this treatment extends equally to PPSIs, so that affiliated entities can coordinate their compliance programs effectively without the PPSI framework creating new information sharing barriers that serve no AML/CFT purpose.

IV. Block, Freeze, and Reject: Technical Capabilities, Smart Contracts, and the Safe Harbor Gap

The GENIUS Act's requirement that PPSIs maintain technical capabilities to block, freeze, and reject impermissible transactions is a critical element in the Proposed Rule. CCI supports the objective underlying Congress's language. The sections below address significant concerns about how OFAC applies these capabilities to smart contract-based stablecoin architectures, the absence of a safe harbor for good-faith blocking actions, and related implementation questions.

A. Scope and Clarity of the Block/Freeze/Reject Obligation (RFC Questions 27, 28, 29)

CCI supports the Proposed Rule's non-prescriptive approach to implementing block, freeze, and reject capabilities. Allowing PPSIs flexibility in how they implement these capabilities — whether through smart contract controls, address-level blocklists, or other mechanisms — is appropriate given the diversity of stablecoin architectures and the pace of technical development in this space.

However, the secondary market scope of this obligation requires further clarification. As currently drafted, it is not sufficiently clear which secondary market scenarios would require a PPSI to act on its blocking capabilities, and which fall outside the obligation given the limiting principle discussed in Section III. CCI recommends that FinCEN issue FAQs or supplemental guidance addressing how the block/freeze/reject obligation applies in specific secondary market contexts, so that PPSIs can design compliant systems without inadvertently over-building or under-building their technical infrastructure.

B. Smart Contract Architecture and the Limits of Transaction Rejection (RFC Question 30)

This section addresses what CCI views as the central technical concern raised by the Proposed Rule: a fundamental mismatch between the regulatory model underlying the block/freeze/reject obligation and the architecture of smart contract-based stablecoin systems.

i. The "Possession or Control Through Smart Contracts" Problem

The NPRM preamble states that PPSIs must have capabilities to identify and block stablecoins traded by blocked persons on the secondary market "when PPSIs exercise possession or control of such stablecoins, including through smart contracts." CCI respectfully challenges the framing that PPSIs exercise control, or facilitates, transactions on the secondary market.

OFAC appears to assert that deploying or operating a smart contract constitutes possession or control of every stablecoin that flows through it on the secondary market. This is a novel legal claim with no established basis in property law, securities law, or existing BSA doctrine. Possession and control are well-developed legal concepts in each of these frameworks, and neither maps cleanly onto the automated, permissionless execution of a smart contract.

FinCEN's 2019 guidance on convertible virtual currencies (FIN-2019-G001) drew a distinction between parties who exercise meaningful discretion over individual transactions and those whose software executes transfers automatically — only the former were treated as intermediaries subject to money transmission obligations.[1] OFAC's 2021 Sanctions Compliance Guidance for the Virtual Currency Industry similarly grounded the blocking obligation in a two-part test:[2] the property must be within a U.S. person's possession or control, and a blocked person must hold an interest in it. A PPSI whose smart contract autonomously processes secondary market transfers among third parties does not exercise the kind of ongoing, transaction-level authority that either agency's prior guidance contemplates as the basis for these obligations.

Accepted at face value, the proposed rule's assertion about smart contracts would mean that a PPSI has custodial control over the payment stablecoin in the secondary market. However, in secondary market transfers, a PPSI has no custody of the stablecoins, holds no private keys, and exercises no discretionary judgment over individual transfers. The smart contract executes the same way regardless of the sender and receiver. Under any consistent reading of "control"

[1] United States Department of the Treasury, Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, May 9, 2019. https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[2] United States Department of the Treasury, Office of Foreign Asset Control, *Sanctions Compliance Guidance for the Virtual Currency Industry*, October 2021. https://ofac.treasury.gov/media/913571/download?inline

grounded in Treasury's own prior guidance, a party that cannot see a transaction coming, cannot evaluate it, cannot stop it, and plays no discretionary role in its execution does not have "control" over it.

The interpretation would mean that a PPSI controls stablecoins in the secondary market; these stablecoins have already been issued in the primary market to the PPSI's customers, and then have been transferred to third parties, who have no customer or contractual relationship with the PPSI, and are transacting freely among themselves — a conclusion that would effectively collapse the primary versus secondary market distinction the NPRM itself draws. It would also set a precedent extending well beyond stablecoins: if operating a smart contract constitutes possession or control of assets flowing through it, that logic could reach anyone deploying a non-discretionary smart contract – software – anywhere in the digital assets ecosystem.

CCI asks FinCEN and OFAC, in final guidance, to reflect the existing 2019 FinCEN and 2021 OFAC guidance, which has been used as the basis for the industry in creating the ecosystem. Applying blocking and rejection obligations to automated, permissionless execution via smart contracts has far reaching implications for Web2 technology as well. CCI further asks FinCEN to confirm that the limiting principle — no obligation to act absent a legal trigger — applies equally where a PPSI's only connection to a secondary market transaction is that its smart contract code processed it.

ii. Technical Feasibility of Secondary Market Rejection

Even setting aside the legal characterization, the infrastructure required to exercise real-time reject actions over secondary market smart contract transactions does not exist in current stablecoin architecture. Blockchain transactions intrinsically are irreversible unlike traditional finance where a bank intermediary can undo a payment transfer. Once a transaction is confirmed on-chain, it cannot be unwound by the issuer.

The smart contracts associated with permitted payment stablecoins as currently implemented function differently from traditional finance processes where a bank sits between sender and receiver and can reject a transaction before it settles. A smart contract executes the transfer autonomously — there is no intermediary moment of discretion where rejection can occur. The only scenario in which the PPSIs has this ability is in dealing with its primary market, where it can stop an outbound transaction to a blocked person.

The GENIUS Act requires PPSIs to have "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations." The statute uses "block, freeze, and reject" as a package but does not explicitly scope this to primary or secondary markets, nor does it define how these capabilities must be implemented. The technical architecture of smart contracts means rejection in the secondary market is not feasible in the way the NPRM implies. Implementing secondary market rejection

capabilities would require PPSIs to build administrative override keys or upgrade mechanisms into their smart contracts — introducing centralization and creating new security vulnerabilities.

CCI recommends that FinCEN clarify that the 'reject' component of the 'block, freeze, and reject' obligation under the GENIUS Act applies only to the primary market and does not require real-time transaction rejection capabilities in the secondary market that current smart contract architecture cannot support. The final rule should confirm that blocklist-based transfer restrictions at the contract level address secondary market activity where full seizure or burn is not architecturally available on the applicable network.

C. The Safe Harbor Gap and Post-Attribution Liability

i. Safe Harbor for Good-Faith Blocking

The Proposed Rule requires PPSIs to maintain capabilities to block, freeze, and reject transactions — including on the secondary market — but provides no safe harbor protecting PPSIs from liability for good-faith blocking actions in the absence of lawful orders, which can be slower moving than crypto transactions. This stands in contrast to the protection FinCEN does provide under § 1033.320(e), which shields PPSIs from civil liability for filing SARs and from liability for failing to notify persons identified in a SAR filing.

The gap is particularly acute given that OFAC administers a strict liability regime. A PPSI that blocks a transaction in good faith — based on available blockchain analytics — has no explicit legal protection. Blockchain analysis data is the only relevant information that a PPSI has access to about the secondary market and such data is only available after transactions settle on-chain. This creates a structural deterrent to proactive blocking that is contrary to the rule's stated objectives.

CCI notes that Treasury's own March 2026 Report to Congress on Innovative Technologies to Counter Illicit Finance Involving Digital Assets recommended that Congress enact a digital asset-specific "hold law" offering a safe harbor to institutions that temporarily and voluntarily hold digital assets during a short-duration investigation, noting that such a law "would be particularly useful for countering illicit finance involving permitted payment stablecoins." CCI supports this recommendation which is currently included in the latest draft of the Digital Asset Markets Clarity Act being considered in Congress,[3] and urges FinCEN to acknowledge the gap explicitly in the preamble to the final rule and note that it requires Congressional action.

ii. Post-Attribution Liability for Pre-Designation Transactions

[3] United States Senate Committee on Banking, Housing, and Urban Affairs, *Digital Asset Market Clarity Act*, July 17, 2025. https://www.banking.senate.gov/imo/media/doc/market_structure_draft.pdf

A related but distinct concern involves transactions processed before a wallet address was officially designated or flagged by blockchain analytics. Under OFAC's strict liability regime, a PPSI could in theory face civil liability for processing a transaction involving a wallet later attributed to a sanctioned person — even where no designation or analytics flag existed at the time of processing.

OFAC's existing guidance recognizes blockchain analytics as a compliance tool and treats a robust sanctions compliance program as a mitigating factor in enforcement. However, PPSIs need explicit confirmation that good-faith reliance on available information at the time of a transaction — with no contemporaneous designation or flag — will not give rise to retroactive civil liability as attribution data develops. CCI recommends that OFAC confirm in the final rule or accompanying guidance that pre-designation transactions processed consistent with a PPSI's effective sanctions compliance program will not be subject to retroactive civil liability solely on the basis of subsequent wallet attribution.

D. Lawful Order Definition and Wallet Address Scope (RFC Question 7)

CCI asks FinCEN to clarify whether wallet addresses are covered as "accounts" for purposes of the lawful order definition. This is not a technical question — it is a foundational operational one. Smart contract-level controls like blocking and seizing operate on wallet addresses, not specific stablecoins within the wallet. PPSIs designing compliant systems need explicit confirmation that a lawful order directed at a wallet address will only trigger obligations that fit within the technical capabilities of common wallet infrastructure.

CCI requests FinCEN to clarify how lawful orders directed at wallet addresses interact with existing account definitions and the PPSI's available technical capabilities, without expanding "account" beyond formal ongoing customer relationships.

CCI also recommends that FinCEN acknowledge and clarify that lawful orders have to pertain to whole wallets rather than partial wallet amounts or specific stablecoins. PPSIs do not have the technical means to block partial amounts.

E. Lawful Order Compliance on the Secondary Market (RFC Question 32)

CCI seeks clarification on how lawful order compliance on the secondary market is expected to work in practice where a PPSI has no direct relationship with the secondary market participant whose assets are subject to the order. The GENIUS Act defines a lawful order as one that "specifies the payment stablecoins or accounts subject to blocking with reasonable particularity" — meaning a valid lawful order must identify specific assets or accounts, not merely a person or entity. CCI asks FinCEN to confirm this explicitly in the final rule. It is an important limiting principle: a PPSI should not be expected to independently attribute secondary market wallet addresses to a named person absent a lawful order that specifically identifies those addresses. Even where a specific

address is identified in a lawful order, a PPSI's ability to act on a permissionless smart contract may be technically constrained in the ways described in Section IV.B. CCI recommends that FinCEN provide guidance on the practical steps a PPSI is expected to take in this scenario and confirm that good-faith efforts to comply — where technical constraints limit the PPSI's ability to act — will be considered in any enforcement context.

F. ATM and Kiosk CTR Filing Responsibility

The Proposed Rule applies CTR obligations to PPSIs scoped to physical currency transactions, anticipating scenarios where stablecoins may be dispensed through retail locations, ATMs, or kiosks. This raises an unresolved question about filing responsibility where a PPSI's stablecoin is involved in a cash transaction conducted through a third-party machine operator.

Under existing FinCEN rules, ATM owners bear the CTR filing obligation for cash transactions aggregating over $10,000 in a single business day. The Proposed Rule does not address how this obligation interacts with a PPSI's CTR obligations where the PPSI is not the machine operator and has no direct relationship with the cash customer. CCI recommends FinCEN confirm that where a PPSI's stablecoin is dispensed or redeemed through a third-party ATM or kiosk, the CTR filing obligation remains with the machine operator consistent with existing rules — and that the PPSI's CTR obligation does not extend to transactions it does not directly process or have visibility into.

G. Implementation Timeline

CCI supports FinCEN's proposed 12-month implementation timeline. This provides sufficient time for PPSIs to establish the required AML/CFT program infrastructure, including written programs, risk assessments, board approval, designated compliance officer, and SAR and CTR obligations, as well as the block and freeze obligations under both the AML/CFT and sanctions compliance programs.

V. Sanctions Compliance Program: Implementation Considerations

CCI supports OFAC's proposal to establish a formal sanctions compliance program requirement for PPSIs under new 31 CFR Part 502. CCI recognizes this as the first time federal law has explicitly mandated that a specific category of U.S. person maintain an effective sanctions compliance program — a significant step that reflects the importance of stablecoins to the U.S. financial system and to national security. While CCI supports this step, the creation of a sanctions program specifically for PPSIs does create imbalance with other financial institutions that do not explicitly have a sanctions compliance program requirement akin to PPSIs. The comments below address practical implementation questions.

A. Best Practices for Sanctions Compliance Program Design (Sanctions RFC Question 3)

PPSIs are not starting from scratch on sanctions compliance. Many current and prospective issuers have already developed sophisticated compliance programs that combine traditional sanctions screening with blockchain-native tools. CCI offers the following observations on best practices that should inform OFAC's approach.

Blockchain analytics tools are a core component of PPSI sanctions compliance in ways that have no direct analog in traditional finance. On-chain data enables PPSIs to screen wallet addresses against OFAC's SDN list, identify addresses associated with sanctioned persons or jurisdictions, and monitor transaction patterns associated with sanctions evasion. API-based integration with OFAC's Sanctions List Service enables real-time screening updates as new designations are issued. CCI notes that Treasury's own March 2026 Report to Congress on Innovative Technologies affirmed blockchain analytics as a critical compliance tool and endorsed API-based sanctions list integration as a best practice — and CCI encourages OFAC to recognize these tools explicitly in its sanctions compliance program guidance for PPSIs.

At the same time, blockchain analytics tools have known limitations. Attribution data is probabilistic, coverage of wallet addresses varies across providers, and obfuscation techniques can reduce confidence in tracing conclusions. OFAC's guidance should acknowledge these limitations and confirm that good-faith reliance on commercially available analytics tools, maintained as part of an effective sanctions compliance program, will be treated as a mitigating factor in enforcement — consistent with OFAC's existing practice in the digital asset space. OFAC should also acknowledge that, particularly in the secondary market, blockchain analytics are *one* data source but should not be considered the *only authoritative* data source, particularly for secondary market actions.

B. Technical Controls for Sanctions-Related Block/Freeze/Reject on the Secondary Market (Sanctions RFC Question 4)

The technical challenges of implementing block/freeze/reject capabilities for sanctions compliance on the secondary market are addressed in detail in Section IV.B above. CCI incorporates that discussion here and adds the following observations specific to the sanctions context.

OFAC's strict liability regime makes the absence of a safe harbor for good-faith blocking particularly consequential. A PPSI that acts on available sanctions screening data — without an associated sanctions action or lawful order — by blocking a secondary market transaction involving a wallet identified as associated with a sanctioned person has no explicit protection from liability, whether that attribution proves correct or incorrect. The combination of OFAC's

strict liability standard, the probabilistic nature of blockchain analytics, and the absence of a safe harbor creates a compliance environment in which the rational response may be to under-block rather than over-block. That outcome is contrary to both OFAC's enforcement objectives and the national security rationale underlying this requirement.

This challenge is meaningfully different from the sanctions screening decisions that traditional financial institutions make. When a bank blocks a transaction based on a sanctions hit, it is acting on activity involving its own customer — a relationship that provides KYC data, account history, and contextual information that helps assess the accuracy of the alert. A PPSI blocking a secondary market transaction has none of that context. The stablecoin may have been issued months earlier and has since traded freely among parties the PPSI has never interacted with. The PPSI is being asked to make a binary enforcement decision based solely on blockchain attribution data, without the account-level context that gives sanctions screening its reliability in traditional finance. CCI is not questioning the value of blockchain analytics as a compliance tool — it is noting that analytics are most effective when combined with account-level context, and that PPSIs lack that context for secondary market activity. A safe harbor or analogous protection for good-faith blocking based on available information is therefore more warranted here than in the traditional finance context, not less.

CCI also notes that OFAC's secondary market requirements, as proposed, may in practice impose obligations closer to customer due diligence than to the blocking and freezing framework FinCEN has established. Requiring PPSIs to identify and act on the sanctions status of secondary market participants with whom they have no direct relationship goes beyond what FinCEN contemplates on the AML/CFT side. CCI asks OFAC to clarify whether its secondary market sanctions obligations are intended to be coextensive with FinCEN's framework or whether they impose additional requirements — and if the latter, to explain the statutory basis for that distinction.

C. Risk Factors for Sanctions Risk Assessments (Sanctions RFC Question 6)

CCI offers the following observations on risk factors PPSIs should consider in designing their sanctions risk assessments. Both on-chain and off-chain factors are relevant.

On the on-chain side: the risk profile of different blockchain networks on which a PPSI's stablecoin is deployed varies, and PPSIs should assess network-specific exposure as part of their sanctions risk assessments. On-chain analytics can support dynamic risk assessment in ways that traditional periodic review cannot, and PPSIs should leverage available tools to monitor transaction activity consistent with their overall risk profile.

On the off-chain side: the geographic distribution of a PPSI's primary market customers and, where available, secondary market activity is a key risk factor, particularly for exposure to

comprehensively sanctioned jurisdictions. Counterparty due diligence on primary market customers — including their own sanctions compliance programs — is an important control given that primary market customers are often the gateway to secondary market activity.

D. Scienter Standard for the Enhanced Penalty Tier (31 CFR 502.301 and 502.401)

OFAC proposes to define "knowingly" for purposes of the enhanced $100,000-per-day civil penalty tier to include circumstances where a PPSI "should have known" of the violation — effectively a negligence standard rather than one requiring actual knowledge or willful blindness. CCI recommends OFAC revise this definition to require actual knowledge or reckless disregard, consistent with how scienter is defined in comparable enforcement contexts.

This is particularly consequential for PPSIs given that OFAC already administers a strict liability regime for underlying sanctions violations. A PPSI can face civil liability for a sanctions violation without any knowledge under that standard. Layering a negligence-based "should have known" definition onto the enhanced penalty tier for sanctions program deficiencies means a PPSI could face both baseline civil liability for an unknowing violation and elevated penalties for a program deficiency it did not intentionally maintain. CCI asks OFAC to clarify that the enhanced penalty tier requires a meaningful showing of actual knowledge or reckless disregard before it is triggered.

VI. Conclusion

CCI appreciates the opportunity to engage with FinCEN and OFAC on this foundational rulemaking. The PPSI AML/CFT and sanctions compliance rule will define the compliance framework for a new regulatory category at a pivotal moment for the stablecoin industry and for U.S. leadership in digital finance. CCI is fully committed to the goals of market integrity, consumer protection, and national security that underlie this rule, and we respectfully submit that a well-calibrated final rule can advance all of these objectives while remaining operationally workable for a diverse and growing industry.

CCI's core requests are straightforward: clarify the boundaries of secondary market obligations and reaffirm the limiting principle stated in the preamble; confirm that Part 1033 applies only to activities directly related to stablecoin issuance and does not displace existing MSB obligations for other activities; address the legal and technical challenges posed by smart contract architecture that make secondary market rejection impractical; acknowledge the safe harbor gap and support Congressional action to fill it; provide OFAC guidance confirming that pre-designation transactions processed in good faith will not give rise to retroactive civil liability; confirm CTR filing responsibility in ATM and kiosk scenarios; revise the scienter standard for the enhanced

penalty tier to require actual knowledge or reckless disregard; and adopt a 12-month implementation timeline that brings this new category of regulated entity under the AML/CFT and sanctions framework.

CCI looks forward to continued engagement with FinCEN and OFAC as this rulemaking progresses and stands ready to serve as a resource, including by providing additional technical or operational information to support the agencies' work. We are committed to being a constructive resource as Treasury works to implement the GENIUS Act in a manner that strengthens the U.S. financial system while enabling responsible innovation.

Respectfully submitted,

Ji Hun Kim
Chief Executive Officer
Crypto Council for Innovation