coinbase

To:

Andrea Gacki, Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, Virginia 22183

Bradley T. Smith, Director
Office of Foreign Assets Control
U.S. Department of the Treasury 1500
Pennsylvania Avenue, NW
Washington, D.C. 20220

June 9, 2026

Submitted electronically via the Federal eRulemaking Portal (www.regulations.gov), Docket No. FINCEN-2026-0100, RIN 1506-AB73.

Re: Joint Notice of Proposed Rulemaking — Permitted Payment Stablecoin Issuer Anti-Money Laundering / Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements

Coinbase Global, Inc. (together with its subsidiaries, "**Coinbase**") respectfully submits this comment in response to the joint Notice of Proposed Rulemaking ("**NPRM**") issued by the Financial Crimes Enforcement Network ("**FinCEN**") and the Office of Foreign Assets Control ("**OFAC**") concerning anti-money laundering ("**AML**"), countering the financing of terrorism ("**CFT**"), and sanctions compliance requirements for Permitted Payment Stablecoin Issuers ("**PPSIs**") under the Guiding and Establishing National Innovation for U.S. Stablecoins ("**GENIUS**") Act.[1]

Coinbase is the most trusted service provider of crypto trading, custody, and infrastructure in the world. Founded in 2012 and publicly listed on the NASDAQ, we offer a secure interface for millions of verified retail and institutional investors globally. We are committed to building an open financial system and are doing so with the strongest regulatory compliance and security protocols available.

Coinbase supports the agencies' goals of combating illicit finance, faithfully implementing the GENIUS Act, and preserving responsible innovation in the U.S. stablecoin market. The comments below are offered in that spirit, with the aim of helping the agencies issue a final rule that is operationally workable, consistent with the statute, and effective in its core mission.

Yours sincerely,

Gerard Monusky

Gerard Monusky
Director, Financial Crimes Legal
Coinbase

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

Executive Summary

The GENIUS Act represents a historic opportunity to cement U.S. leadership in digital assets by bringing stablecoins into a clear, federally regulated perimeter. Coinbase shares the agencies' commitment to keeping illicit actors out of this ecosystem. However, for this regulatory framework to succeed — and to prevent the market from being driven offshore — the final rule must reflect the technological reality of how public blockchains actually operate.

The single most important principle in this rulemaking[2] is preserving the distinction between primary market and secondary market activity. When a PPSI mints or redeems a token, it acts akin to a traditional financial intermediary: it knows its customers, performs due diligence, and maintains an ongoing relationship. But once a token enters general circulation on a public blockchain, the PPSI has no contractual relationship with downstream token holders. Attempting to force traditional, account-based compliance obligations onto these secondary market transactions is technologically unworkable and creates massive data privacy risks. Further, extending Know-Your-Customer ("**KYC**") and suspicious activity report ("**SAR**") obligations to secondary market holders would divert scarce resources away from the primary market perimeter, diluting the overall effectiveness of the compliance program where the PPSI has the context to perform meaningful due diligence, and incentivizing users to operate outside the regulated U.S. financial system.

The GENIUS Act reflects this distinction and directs the agencies to tailor AML and sanctions rules to the size, complexity, business model, and risk profile of the regulated issuer.[3] In practical terms, this is a "gatekeeper" model: the PPSI identifies and performs due diligence on its own mint and redeem counterparties at the regulated on- and off-ramps, while downstream circulation remains governed by sanctions controls, analytics, and other risk-based measures appropriate to parties outside the PPSI's customer perimeter.

Coinbase supports the proposal's risk-based calibration and urges the agencies to preserve that tailoring throughout the final rule. Our principal recommendations to accomplish that are as follows:

- **Account scope**. The definition of an "account" is properly limited by the term "customer" to reach only a PPSI's direct mint and redeem counterparties. The agencies should confirm this reading in the final rule's preamble to prevent over-collection of sensitive personal data from secondary market holders and to avoid creating unnecessary "honeypots" of identity information susceptible to cybercriminals.

---

[2] Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, Joint Notice of Proposed Rulemaking, Docket No. FINCEN-2026-0100, RIN 1506-AB73 (FinCEN/OFAC 2026) (hereinafter "NPRM").

[3] *See* GENIUS Act § 4(a)(5)(B) (directing that regulations be "tailored to the size and complexity" of PPSIs).

- **SAR carve-out.** The agencies should finalize and strengthen the SAR carve-out for secondary market smart-contract transfers and decline to adopt a "knows or has reason to know" standard. A broader standard would force PPSIs into defensive, automated filing — flooding FinCEN with low-signal SARs that add nothing beyond what is already visible on the public ledger and degrading the utility of the Bank Secrecy Act ("**BSA**") database.

- **Civil safe harbor.** PPSIs that act in good faith to comply with the final rule, execute lawful orders, or follow OFAC directives should not face private civil liability for those actions. The agencies further should treat good-faith compliance as a significant mitigating factor in supervision and enforcement and support a legislative solution modeled on the BSA SAR safe harbor.

- **Travel Rule.** A PPSI-specific Travel Rule and Recordkeeping Rule would be valuable if it confirms the existing scope of those obligations under the BSA, in that they only apply when the PPSI actually serves as the transmittor's or recipient's financial institution. Meaning such an obligation would only apply in primary market mint and redeem transfers — not in secondary market, peer-to-peer transfers, in which the PPSI is not a party.

- **Supervisory credit for blockchain analytics.** The final rule should extend the mitigating-factor framework beyond enforcement actions to routine examinations and supervisory ratings. Because blockchain analytics are inherently probabilistic, the rule should reward good-faith use of these tools as a compliance enhancement.

- **Lawful orders.** To protect innocent consumers whose assets sit in commingled or omnibus wallets, the definition of "lawful order" should clarify that the statutory requirement of "reasonable particularity" is satisfied only by identifying the specific wallet address(es) subject to the order.

I. The Scope of "Accounts"

NPRM Question B(5): *Are FinCEN's proposed definitions sufficiently clear? Should the definitions be expanded or narrowed in any respect? Should FinCEN define additional terms or amend additional existing terms?*

NPRM Question C(17): *To what extent should PPSIs consider information about secondary market transactions as part of their customer due diligence processes?*

Recommendation: FinCEN should confirm that the proposed "account" definition reaches only the PPSI's mint and redeem counterparties and does not extend to secondary market holders of the issued payment stablecoin.

The NPRM correctly preserves the distinction between primary and secondary market activity. Crucially, the NPRM proposes to amend § 1010.230(c) to define a PPSI "account" as a "formal relationship between a customer and a permitted payment stablecoin issuer."[4] Under longstanding BSA regulations, a "customer" is strictly a person who establishes a direct, formal relationship with a financial institution.[5]

Applied to the stablecoin ecosystem, this means a PPSI's "accounts" are limited to the specific counterparties that directly mint and redeem the stablecoin with the issuer — typically, the party that mints by depositing fiat and the party that redeems by returning the token. The definition rightly excludes secondary market holders who acquire the token downstream. Such holders have not entered into any account agreement with the PPSI and have no contractual relationship with the issuer, therefore the PPSI lacks both the practical ability and any legal basis to treat them as account holders.

That reading is also consistent with the structure of existing BSA rules, which tie customer-identification and account-based obligations to formal relationships established with the financial institution itself.[6] Nothing in those existing frameworks suggests that an issuer must identify every downstream holder of an instrument once it is in general circulation. This is further reinforced by the GENIUS Act itself, which expressly preserves certain direct transfers and self-custodial wallet activity,[7] underscoring Congress's recognition that downstream circulation is distinct from issuer-side intermediation.

Because the regulatory text itself is already properly scoped, no amendment is necessary. A preamble confirmation in the final rule, however, would provide meaningful value. Examiners and supervised institutions would have a clear point of reference, PPSIs would not be pressured to over-collect identity information on persons who are not their customers, and the final rule would foreclose interpretations that would, in effect, extend BSA obligations to a population Congress did not designate.

A preamble confirmation also serves a substantial privacy and information-security interest. Customer identification files maintained by financial institutions are concentrated repositories (or "honeypots") of sensitive personal information and recurring targets of sophisticated cyberattacks. Expanding customer-identification obligations beyond a PPSI's

---

[4] *See* NPRM § VI.C.5 (proposing to amend 31 CFR § 1010.230(c) to include PPSI-specific "account" language).
[5] *See, e.g.*, 31 CFR § 1020.100(b) (defining a bank "customer" as, *inter alia*, "a person that opens a new account"); 31 CFR § 1020.100(a) (defining "account" as a "formal banking relationship established to provide or engage in services, dealings, or other financial transactions"). *See also* 31 CFR § 1023.100(a), (d) (parallel definitions for broker-dealers). By using these established definitions in the PPSI context, FinCEN correctly imports the traditional requirement of a direct, formal relationship.
[6] *See id. See also* 31 CFR § 1020.220 (providing for bank customer identification program requirements tied to customers opening accounts); 31 CFR § 1023.220 (establishing parallel customer identification program requirements for broker-dealers).
[7] *See* GENIUS Act § 3(h).

actual customers would multiply these repositories without a corresponding compliance benefit.

Overcollection is not merely inefficient; it also creates severe security risks and degrades AML effectiveness by flooding compliance teams with low-value data and diverting focus away from the primary market perimeter, where the PPSI possesses the customer relationship necessary to conduct meaningful due diligence. The BSA was designed to detect criminal conduct in established customer relationships, not to force an issuer to identify every downstream holder of a bearer-like instrument once it enters general circulation.

For these reasons, we recommend that FinCEN include the following clarification in the preamble to the Final Rule:

> FinCEN confirms that the term "account" as defined in § 1010.230(c) extends only to those persons who maintain a formal mint-and-redemption relationship with the Permitted Payment Stablecoin Issuer. Secondary market holders who acquire a payment stablecoin without entering into such a relationship are not "customers" of the issuer for purposes of this part, and the issuer is not required to identify, monitor, or verify the identity of such persons. Nothing in this part is intended to require a Permitted Payment Stablecoin Issuer to apply customer identification, customer due diligence, or account-based suspicious activity reporting obligations to secondary market holders.

II. SAR Filings and the § 1033.320(g) Smart-Contract Carve-Out

NPRM Question F(35): *Is FinCEN's proposal clear regarding SAR obligations relating to secondary market activity? If not, why not and how can it be improved?*

NPRM Question F(39): *Should FinCEN reconsider its decision not to impose any SAR obligation with respect to secondary market activity? In what circumstances would secondary market reporting be most beneficial and how burdensome would such a reporting obligation be? For example, should PPSIs be required to report secondary market suspicious activity but only at a higher standard than in primary market transactions, such as requiring reporting only when a PPSI "knows" a transaction meets specified criteria?*

Recommendation: FinCEN should affirm and strengthen the suspicious activity reporting carve-out for smart-contract transfers that a PPSI did not initiate, authorize, or otherwise facilitate. FinCEN should decline to adopt the broader "knows or has reason to know" framing.

In the NPRM, FinCEN proposes at § 1033.320(g) to relieve PPSIs of the obligation to file a SAR with respect to a secondary market smart-contract transfer of a payment stablecoin that the PPSI did not initiate, authorize, or otherwise facilitate. FinCEN then asks whether that carve-out is appropriate and whether the agency should reconsider it in favor of an elevated "knows or has reason to know" standard.

FinCEN's preliminary judgment to carve out secondary market transfers makes sense and should be finalized. A PPSI generally cannot be expected to file a useful SAR on a secondary market transfer that it did not intermediate and for which it lacks customer context. Public-ledger visibility may show that a transfer occurred, but it does not by itself provide the identity, relationship history, commercial context, or purpose-of-activity information that makes a SAR genuinely useful to law enforcement. While advanced blockchain analytics and artificial intelligence are highly effective at optimizing AML programs for an issuer's direct customers, applying these tools to public-ledger data alone — without primary market context — yields high volumes of low-value, defensive reporting.

Indeed, federal law enforcement already employs sophisticated blockchain analytics to trace secondary market activity and, where appropriate, to identify and approach the primary market PPSI or other intermediary that can furnish the underlying customer context. That existing capability works precisely because it pairs public-ledger observability with targeted requests to the party holding the relevant records. A standalone secondary market reporting obligation would not enhance this process; it would degrade it, burying genuinely high-value signals in a flood of low-value filings.

Further, adopting a "knows or has reason to know" standard would be highly detrimental to FinCEN's core mission. Because blockchain analytics tools continuously update and can retroactively flag previously unflagged addresses, a "reason to know" standard would expose PPSIs to liability for transactions that appeared unremarkable at the time but later become associated with risk. To avoid regulatory scrutiny, PPSIs would be forced into massive, automated defensive filing, flooding FinCEN with thousands of low-signal SARs that contain no actionable intelligence beyond what is already visible on the public ledger. This would severely degrade the utility of the BSA database. Additionally, investigating and processing these low-signal, secondary market reports would drain the very resources that a PPSI relies upon to rigorously monitor its direct mint-and-redeem counterparties — subverting the risk-based allocation of resources that is the foundation of an effective AML program.

To prevent this, the final rule should confirm that a PPSI's routine compliance activities — such as utilizing blockchain analytics, or screening against OFAC lists — do not convert a secondary market transfer into a transaction "conducted by, at, or through" the PPSI.[8] A PPSI should not be required to stand up separate monitoring and investigation systems for

---

[8] *See* 31 CFR § 1020.320(a)(2) (limiting a bank's SAR-reporting obligations to transactions "conducted or attempted by, at, or through" the bank, rather than downstream, off-platform transactions); 31 CFR § 1023.320(a)(2) (same for broker-dealers); 31 CFR § 1022.320(a)(2) (same for money services businesses).

secondary market activity outside the bounds of specific legal obligations (e.g., OFAC sanctions or lawful orders). Treating public-ledger visibility as constructive participation would penalize institutions that invest in advanced analytics.

Proposed § 1033.320(g)	
FinCEN/OFAC Proposed Text	**Coinbase Proposed Revision**
§ 1033.320(g) Transaction. A transaction, for purposes of § 1033.320, 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.	§ 1033.320(g) Transaction. A transaction, for purposes of § 1033.320, 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. For purposes of this paragraph, none of the following activities, taken alone or in combination, constitutes conducting, attempting, or otherwise facilitating a transaction: observing the transaction on a public blockchain; performing sanctions screening against published government lists; complying with a lawful order or directive of the Office of Foreign Assets Control; or applying blockchain analytics to assess risk.

III. Civil Safe Harbor

OFAC Sanctions Question 5: *To what extent does the proposed rule appropriately afford PPSIs flexibility to determine how to implement the technical capability to block, freeze, and reject transactions, consistent with their business models, technologies, and risk profiles?*

NPRM Question D(27): *Should FinCEN refine or clarify the obligation related to having the technical capabilities to block, freeze, and reject impermissible transactions?*

Recommendation: The agencies should: (i) treat good-faith compliance with the final rule, lawful orders, and OFAC directives as a significant mitigating factor in supervision and enforcement; (ii) acknowledge in the final rule's preamble the absence of statutory civil liability protection for PPSIs executing block, freeze, reject, seize, and burn obligations, and the resulting need for legislative action; and (iii) support legislation creating a civil safe harbor modeled on the existing BSA SAR safe harbor.

The final rule will require PPSIs to block, freeze, reject, seize, and burn assets and transactions on tight timeframes. This creates a dilemma: a PPSI that fails to act when action is legally required faces regulatory exposure, while a PPSI that does act faces potential private litigation from affected holders challenging the basis, timing, or duration of the action. Congress recognized a similar structural problem in the BSA context and addressed it through the SAR safe harbor at 31 U.S.C. § 5318(g)(3), which shields financial institutions and their personnel from civil liability for good-faith SAR-related disclosures.

PPSIs operating in a faster and more publicly visible onchain setting warrant comparable protection when executing these obligations. The clearest path to that protection is legislation, and Coinbase encourages the agencies to support such legislation as part of the final rulemaking. The protection should cover four categories of action: (i) good-faith compliance with the AML, CFT, and sanctions requirements of the final rule; (ii) action taken pursuant to a lawful order; (iii) action taken pursuant to an OFAC directive; and (iv) action taken during the period preceding the rule's effective date to bring the PPSI into compliance. This fourth category is particularly important, as the period between issuance of the final rule and its effective date is when good-faith compliance investments are most vulnerable to second-guessing.

In the absence of statutory protection, the agencies should take two steps within their existing authority. First, the final rule's preamble should expressly acknowledge that PPSIs executing required block, freeze, reject, seize, and burn actions in good faith currently lack the statutory civil liability protection that Congress provided to other financial institutions for SAR-related disclosures, and that this gap warrants legislative attention. Second, the agencies should state in the preamble that good-faith actions to comply with the final rule — including blocking, freezing, etc., and good-faith decisions made during the rule's implementation period — will be treated as significant mitigating factors in supervision and enforcement.

To the extent the agencies conclude they have authority to codify civil liability protection by regulation, they should do so. The proposed regulatory text below sets out language the agencies could adopt.

Proposed § 1033.241 (FinCEN)	
FinCEN/OFAC Proposed Text	**Coinbase Proposed Revision**
[No existing text. Coinbase proposes adding § 1033.241.]	§ 1033.241 Civil safe harbor. (a) No Permitted Payment Stablecoin Issuer, and no director, officer, employee, or agent of a Permitted Payment Stablecoin Issuer, shall be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any

	contract or other legally enforceable agreement, for any action taken in good faith to comply with this part, with a lawful order as defined in § 1010.100(rrr), or with any directive of the Office of Foreign Assets Control. (b) Action taken during the period preceding the effective date of this part to bring a Permitted Payment Stablecoin Issuer into compliance with this part shall be deemed to have been taken in good faith for purposes of paragraph (a).

Proposed § 502.301 (OFAC)	
FinCEN/OFAC Proposed Text	**Coinbase Proposed Revision**
[No existing text; Coinbase proposes adding § 502.301.]	§ 502.301 Civil safe harbor. No Permitted Payment Stablecoin Issuer, and no director, officer, employee, or agent of a Permitted Payment Stablecoin Issuer, shall be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement, for any action taken in good faith to comply with this part, with any directive of the Office of Foreign Assets Control, or with any lawful order as defined in 31 CFR § 1010.100(rrr).

IV. Travel Rule — Proposed § 1033.410

NPRM Question G(41): *Would Recordkeeping and Travel Rule obligations for PPSIs and other financial institutions be clearer if FinCEN codified a PPSI-specific Recordkeeping and Travel Rule in part 1033?*

Recommendation: FinCEN should codify a PPSI-specific Recordkeeping and Travel Rule that confirms these obligations apply where a PPSI acts as the transmittor's or recipient's financial institution, consistent with existing BSA rules.

FinCEN asks whether codifying a PPSI-specific Recordkeeping and Travel Rule would make those obligations clearer. A PPSI-specific rule would be beneficial, provided it confirms that the obligations attach where the PPSI actually serves as the transmittor's or recipient's financial institution.

Under the existing rules, obligations apply specifically to the "transmittor's financial institution" and the "recipient's financial institution."[9] For a PPSI, those roles arise in the issuance-and-redemption context only — i.e., when the PPSI transfers fiat or stablecoins to its direct counterparty financial institution. In a secondary market transfer between two unhosted wallets, or between an unhosted wallet and a custodial wallet at a third-party platform, the PPSI is neither the transmittor's nor the recipient's financial institution. The PPSI deployed the smart contract on which the transfer settles, but the transfer itself is between other parties and involves no instruction to the PPSI to pay a recipient. Because there is no transmission instruction directed to the PPSI, the core prerequisite for a "transmittal of funds" under the BSA does not exist.

Codifying a PPSI-specific rule that confirms this scoping would resolve ambiguity for PPSIs and their counterparties without changing the substance of the existing Travel Rule. It would also avoid the operational and legal complications that would arise from any interpretation extending Travel Rule obligations to transfers in which the PPSI is not the transmittor's or recipient's financial institution.

For primary market transfers that are properly subject to the Travel Rule, the digital asset industry has demonstrated its ability to build and operate compliant information-sharing infrastructure. Coinbase helped organize the Travel Rule Universal Solution Technology ("**TRUST**") network, an industry consortium that facilitates compliant information sharing among digital asset firms. The success of TRUST and similar networks indicates that, when Travel Rule obligations are correctly tied to the institutions actually conducting the transfers, industry can deliver effective compliance without prescriptive technical mandates.

Proposed § 1033.410	
FinCEN/OFAC Proposed Text	**Coinbase Proposed Revision**
[No existing text. Coinbase proposes adding § 1033.410.]	§ 1033.410 Travel Rule application. (a) A Permitted Payment Stablecoin Issuer shall comply with the requirements of § 1010.410(e) and § 1010.410(f) when acting as the transmittor's financial institution, an intermediary financial institution, or the recipient's financial institution in a transmittal of funds.

[9] *See* 31 CFR § 1010.410(e), (f).

	(b) Rule of Construction.—For purposes of this section, a Permitted Payment Stablecoin Issuer does not act as a transmittor's financial institution, an intermediary financial institution, or a recipient's financial institution with respect to a secondary market transfer of a payment stablecoin between persons who do not maintain an account with the Permitted Payment Stablecoin Issuer.

V. Supervisory Credit for Blockchain Analytics

NPRM Question C(26): *FinCEN welcomes comment on how the Director of FinCEN may consider the performance of innovative activities that produce demonstrable outputs under the proposed supervision and enforcement framework.*

Recommendation: FinCEN should amend the rule to ensure that the use of proactive blockchain analytics and other innovative compliance tools is credited during routine examination ratings, not just during enforcement actions.

FinCEN asks how it should consider the performance of innovative activities under its supervision framework. As a starting point, the proposed § 1033.221(d) takes a highly constructive step: it directs FinCEN to consider a PPSI's "proactive analytics" and "innovative activities," such as advanced monitoring tools, as mitigating factors. Coinbase strongly supports this provision.

The proposed credit reflects an important reality: blockchain analytics meaningfully expand what financial institutions can detect and report. Unlike traditional AML monitoring — which is typically limited to a financial institution's own customers and own ledger — blockchain analytics enable PPSIs to draw on a transparent, immutable transaction record that extends well beyond their own operational perimeter. That transparency, combined with the analytical capabilities now built on top of it, allows for real-time risk scoring, dynamic counterparty assessment, and rapid identification of illicit activity in ways that traditional financial monitoring cannot match. Encouraging PPSI investment in these tools serves FinCEN's mission directly: better detection, faster interdiction, and more useful reporting.

Crediting good-faith use of analytics is also important because blockchain attribution is inherently probabilistic. Analytics providers rely on evolving heuristics, meaning a wallet address's risk score or cluster affiliation can change over time as new data emerges. PPSIs should not face supervisory second-guessing because a transaction that appeared unremarkable at the time was later flagged when an analytics provider updated its model.

The agencies should evaluate these innovative compliance tools by reference to the PPSI's testing, validation, ongoing performance monitoring, and demonstrable outputs, rather than by whether the tool mirrors legacy controls. Where a PPSI has established a reasonably designed program, isolated, technical, or immaterial implementation issues arising from the good-faith use of these advanced tools should not support significant supervisory criticism or enforcement.

The proposed § 1033.221(d) provides this credit only in the context of an "enforcement action or significant AML/CFT supervisory action." But routine examinations and supervisory ratings are often the most consequential and frequent regulatory touchpoints for most PPSIs. A PPSI that invests heavily in blockchain analytics or other advanced detection tools should receive credit for those investments in the ordinary supervisory process, not only when the institution is already facing enforcement exposure. And because routine examinations are conducted by the agencies to which FinCEN has delegated examination authority under § 1010.810, the obligation to consider these factors should extend to those examining authorities as well as to FinCEN itself.

Extending the § 1033.221(d) factors to examination ratings and routine supervisory engagements across all relevant examining authorities would meaningfully incentivize the kind of compliance innovation the rule is designed to encourage — and would align FinCEN's supervisory posture with its broader policy interest in seeing PPSIs adopt the most effective AML/CFT tools available.

Proposed § 1033.221(d)	
FinCEN/OFAC Proposed Text	**Coinbase Proposed Revision**
§ 1033.221(d) FinCEN considerations. In determining whether to take an AML/CFT enforcement action or significant AML/CFT supervisory action, or when reviewing a proposed action by a primary Federal payment stablecoin regulator under paragraph (c) of this section or applicable regulations under title 12 of the Code of Federal Regulation, the Director, FinCEN shall consider: (1) The factors under 31 U.S.C. 5318(h)(2)(B), as applicable to actions concerning the AML/CFT program requirements under § 1033.210; (2) The extent (if any) to which the permitted payment stablecoin issuer,	§ 1033.221(d) FinCEN and Examining Authority considerations. In determining whether to take an AML/CFT enforcement action or significant AML/CFT supervisory action, in conducting compliance examinations and assigning supervisory ratings, or when reviewing a proposed action by a primary Federal payment stablecoin regulator under paragraph (c) of this section or applicable regulations under title 12 of the Code of Federal Regulations, the Director, FinCEN, and any agency acting pursuant to delegated examination authority under § 1010.810, shall consider: (1) The factors under 31 U.S.C. 5318(h)(2)(B), as applicable to actions

where appropriate in light of its size, complexity, and risk profile, has advanced the AML/CFT priorities by providing highly useful information to law enforcement authorities or national security officials, conducting proactive analytics, or performing other innovative activities producing demonstrable outputs evincing the effectiveness of the permitted payment stablecoin issuer's AML/CFT program (including effective use of artificial intelligence, federated learning, and other advanced monitoring tools); and (3) Any other factor the Director, FinCEN deems appropriate, including the permitted payment stablecoin issuer's size, complexity, and risk profile, and, as relevant, where the permitted payment stablecoin issuer's low-risk customers or limited business activities naturally limits the extent to which the permitted payment stablecoin issuer can meaningfully contribute to AML/CFT priorities.	concerning the AML/CFT program requirements under § 1033.210; (2) The extent (if any) to which the permitted payment stablecoin issuer, where appropriate in light of its size, complexity, and risk profile, has advanced the AML/CFT priorities by providing highly useful information to law enforcement authorities or national security officials, conducting proactive analytics, or performing other innovative activities producing demonstrable outputs evincing the effectiveness of the permitted payment stablecoin issuer's AML/CFT program (including effective use of artificial intelligence, federated learning, and other advanced monitoring tools); and (3) Any other factor the Director, FinCEN, or the examining authority deems appropriate, including the permitted payment stablecoin issuer's size, complexity, and risk profile, and, as relevant, where the permitted payment stablecoin issuer's low-risk customers or limited business activities naturally limits the extent to which the permitted payment stablecoin issuer can meaningfully contribute to AML/CFT priorities.

VI. Lawful Order Definition

NPRM Question B(7): *Is FinCEN's proposed definition of "lawful order" sufficiently clear? Should FinCEN further define any terms within "lawful order"? Should FinCEN, for example, specify that "accounts" for purposes of lawful orders include any number or identifier used to identify a holder of a payment stablecoin, including a wallet address?*

Recommendation: FinCEN should finalize its proposed definition of "lawful order," which correctly tracks the GENIUS Act, with one important clarification: the final rule should expressly state that the statutory requirement of "reasonable particularity" is satisfied only by identifying the exact, specific wallet address(es) subject to the order.

Proposed § 1010.100(rrr) creates the defined term "lawful order" that anchors a PPSI's obligations under proposed § 1033.240(b) to comply with such orders. FinCEN's proposed definition closely tracks the statutory definition of "lawful order" in Section 2(16) of the GENIUS Act, with limited modifications.[10] Coinbase supports this alignment.

The GENIUS Act and the proposed rule require a lawful order to specify the "payment stablecoins or accounts" subject to the order with reasonable particularity. However, the traditional concept of an "account" does not neatly map to the technical realities of public blockchains, where assets are held in wallet addresses. To make this definition operationally workable for PPSIs, the final rule must bridge the gap between the statutory text and onchain mechanics. Specifically, we recommend that FinCEN add a clarifying provision to the definition of "lawful order" expressly stating that identifying the specific wallet address satisfies the requirement for "reasonable particularity."

The particularity requirement is crucial. An instruction directed at an open-ended class of addresses merely "associated with" a type of conduct, or at an unnamed "cluster," should not satisfy the statutory standard. Identifying specific wallet addresses is properly the function of the issuing authority, which has access to the investigative record and the analytical resources to make those determinations with confidence. If an investigating authority has identified a cluster of addresses controlled by a bad actor, the resulting lawful order should enumerate those specific addresses.

This particularity limitation is especially important where payment stablecoins are held through omnibus, pooled, or custodial wallets operated by digital asset platforms. In those settings, overbroad or vaguely defined instructions can inadvertently freeze the assets of innocent third parties.[11] The final rule must balance the need to execute lawful orders with the need to protect non-subject customers and shield PPSIs from liability.

Proposed 31 C.F.R. § 1010.100(rrr)	
FinCEN/OFAC Proposed Text	**Coinbase Proposed Revision**
§ 1010.100(rrr) Lawful order. A lawful order is 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:	§ 1010.100(rrr) Lawful order. A lawful order is 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:

[10] *See* proposed 31 CFR § 1010.100(rrr) (substituting the GENIUS Act's enumerated "person" language for the statutory term "person" to avoid conflicts with FinCEN's existing definition of "person" at 31 CFR § 1010.100(mm)); *see also* NPRM § VI.C.1.vii.

[11] Digital asset exchanges and custodians frequently utilize "omnibus" wallets, commingling the assets of thousands of innocent retail customers into a single onchain address for operational efficiency. An order that fails to identify a target with absolute particularity risks unlawfully freezing the assets of every customer in the pool.

• (1) Requires an individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated, to seize, freeze, burn, or prevent the transfer of payment stablecoins it issued; • (2) Specifies the payment stablecoins or accounts subject to blocking with reasonable particularity; and • (3) Is subject to judicial or administrative review or appeal as provided by law.	• (1) Requires an individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated, to seize, freeze, burn, or prevent the transfer of payment stablecoins it issued; • (2) Specifies the payment stablecoins or accounts subject to blocking with reasonable particularity; and • (3) Is subject to judicial or administrative review or appeal as provided by law. • (4) For purposes of paragraph (2), reasonable particularity with respect to payment stablecoins or accounts requires the identification of the specific, individual wallet address or a finite, enumerated list of specific wallet addresses.

Conclusion

Coinbase appreciates the opportunity to comment on this important rulemaking and welcomes continued engagement with FinCEN and OFAC staff on the operational implementation questions raised by the recommendations above.

The GENIUS Act represents a landmark opportunity to onshore stablecoin innovation, protect U.S. consumers, and establish the United States as the undisputed global leader in digital assets. However, the success of this framework depends entirely on whether the implementing regulations are operationally workable for the institutions expected to adopt them. Adhering to the primary market perimeter will produce a final rule that is effective in combating illicit finance, faithful to the GENIUS Act, and workable for the responsible PPSIs on which the U.S. payment stablecoin market will depend.