June 9, 2026

Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Office of Foreign Assets Control
U.S. Department of the Treasury
Treasury Annex / Freedman's Bank Building
1500 Pennsylvania Avenue NW
Washington, DC 20220

ATTN: FINCEN-2026-0100

Re: Comments on FinCEN and OFAC Notice of Proposed Rulemaking: AML/CFT and Sanctions Compliance Program Requirements for Permitted Payment Stablecoin Issuers

Dear Director Gacki and Director Smith:

Andreessen Horowitz ("a16z" or "we") appreciates the opportunity to submit this comment in response to the joint proposed rule to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins ("GENIUS") Act. The FinCEN and OFAC staff have taken a thoughtful approach to implementing the GENIUS Act, and we applaud the staffs' commitment to soliciting information from the public through a transparent process, encouraging innovation in payment stablecoins while also providing an appropriately tailored regime to protect consumers, mitigate potential illicit finance risks, and address financial stability risks.

I. About a16z

A16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on AI, bio and healthcare, consumer, crypto, enterprise, fintech, games, infrastructure, and companies building toward American dynamism. A16z currently has more than $100 billion in assets under management across multiple funds, with more than $9.8 billion in committed capital for crypto funds. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch Internet businesses. We are deeply committed to the development of an appropriate legal and regulatory framework for digital assets like stablecoin. We believe such a framework is critical to fostering innovation while protecting market participants. To that end, we hope that our observations, drawn from our

deep experience, can be of assistance to FinCEN and OFAC in drafting the final rule.

II. Executive Summary

In this comment to the Proposed Rule, we have focused on specific issues where we believe we can provide the most useful insights.

- Parts III.A and III.B outline concerns regarding ambiguities in the definition of "Payment Stablecoin," especially as they pertain to stablecoins not used for retail payment.
- Part III.C addresses several issues regarding the definition of "final order" – namely, ensuring further clarity as to what constitutes "finality" in the context of appealable orders, and that such "final orders" should specify the wallet address or addresses to be covered by the order. We also describe the significant risks and burdens placed upon PPSIs for good-faith compliance with such orders and suggest possible ways to address those risks.
- Part IV discusses the specific substantive obligations. Part IV.A agrees with FinCEN's proposal to exempt PPSIs from the MSB category, but we further suggest that all such activities of the PPSI should fall under 31 C.F.R. 1033 (the PPSI rules), rather than having a company being subject to two separate sets of regulations.
- Part IV.B addresses how the rules, both for FinCEN and OFAC, should apply to issuers only at the time of issuance and redemption and should not extend to PPSIs for secondary market activity.
- Part IV.C discusses the OFAC Sanctions Compliance Program Rule, a novel concept, given that no other financial institution has such a rule. While the GENIUS Act calls for some SCP, the statute only calls for such SCPs to be effective, include verification of sanctions lists, and be tailored. We respectfully submit that the Proposed Rule goes far beyond the statute, and thus should be limited. In addition, we suggest a two-year implementation period for the development of such programs.
- Part IV.D recommends that Treasury authorize and encourage the use of innovation to combat illicit finance and to meet BSA and OFAC obligations, and we describe some innovations particularly well-suited for these objectives.
- As a corollary to Subpart D, Part IV.E emphasizes a concern that is critical to adoption and consumer protection of stablecoins generally: privacy. We urge that the Final Rule should account for such concerns, including by establishing explicit protections for privacy-preserving technologies and rescinding FinCEN's pending mixing-related special measure.

- Finally, Part IV.F addresses risk assessment requirements and the beneficial ownership rules, which have not yet been formally proposed by Treasury.

III. Clarifying Core Concepts

The Proposed Rule requests comments on numerous terms defined in the Act. Clarifying the concepts discussed below is essential not only for entities directly regulated by GENIUS, but also for users of payment stablecoins, technology investors, and developers. Clarity for these terms is critical in that it will determine the scope of important regulatory categories, establish the GENIUS Act's covered activities, and set consequences for non-compliance.

A. The Final Rule Should Make Clear that Non-Payment Stablecoins are Outside the Scope of the GENIUS Framework.

Not all stablecoins used for payment are "payment stablecoins" subject to the Act. This fact is acknowledged by the Act itself, requiring the Department of the Treasury to conduct a study exploring the varieties and potential complexities of "non-payment stablecoins," and provide a report to the Senate Committee on Banking, Housing, and Urban Affairs and the House Committee on Financial Services.[1] Indeed, we look forward to reviewing this study, and are available as an expert resource on any and all covered topics, including (A) the benefits and risks of technological design features; (B) the participants in non-payment stablecoin arrangements; (C) utilization and potential utilization of non-payment stablecoins; (D) the nature of reserve compositions; (E) types of algorithms being employed; (F) governance structure, including aspects of decentralization; (G) the nature of public promotion and advertising; and (H) the clarity and availability of consumer disclosures. Therefore, it would be contrary to Congressional intent to conflate "non-payment stablecoins" and "payment stablecoins" for purposes of this regulatory framework.[2]

[1] GENIUS Act, Pub. L. No. 119–27, § 14, 139 Stat. 460.

[2] We specifically refer FinCEN and OFAC to our previous submissions, which explain the technical foundations and benefits of decentralized stablecoins, and why the GENIUS Act's threshold definitions and core prohibitions exclude decentralized stablecoins from the Act's scope. Miles Jennings et al., *a16z Response to Treasury Advance Notice of Proposed Rulemaking; GENIUS Act Implementation Comments*, Andreessen Horowitz (Nov. 4, 2025) at 2–6, https://tinyurl.com/ykfazdbd; Miles Jennings et al., *a16z Response to Notice of Proposed Rulemaking: Implementing the GENIUS Act for the Issuance of Stablecoins by Entities Subject to the Jurisdiction of the OCC*, Andreessen Horowitz (May 1, 2026) at 19–21, https://tinyurl.com/txf5s7v4.

B. The Final Rule Should Address Critical Ambiguities in the Definition of "Payment Stablecoin."

Treasury and FinCEN should address critical ambiguities in the definition of "payment stablecoin" that warrant clarification. A payment stablecoin is described as a digital asset that, among other elements, "is, or is designed to be, used as a means of payment or settlement."[3] This element potentially invites arbitrary and subjective interpretation that could chill experimentation and innovation with digital assets. For example, it is unclear whether being "designed" for a use is based on the subjective intent of the creator of the digital asset or the asset's objective design characteristics (e.g., technical capabilities). Moreover, the definition does not specify what level or manner of use is required to establish that a digital asset "is used as a means of payment or settlement" (e.g., is one such transaction sufficient, or must it be the primary use of the stablecoin among users as whole?). Conversely, this criterion leaves open the possibility that sufficiently many stablecoin holders might begin to use a stablecoin for another purpose (e.g., as a store of value), such that the digital asset could later fall outside of the Act's definition.

The Proposed Rule's definition of "payment stablecoin" could also be misconstrued in a manner that raises uncertainty as to whether it encompasses "arcade tokens," a category of digital assets that function as currencies within a contained digital ecosystem—such as airline miles, credit card rewards points, or digital gold in a video game—and that are intended primarily to facilitate user interactions, access to features, or the redemption of products or services, rather than to serve as general-purpose payment or settlement instruments.[4] By design, arcade tokens are limited in scope and often do not represent a fixed amount of monetary value. For this reason, arcade tokens do not meet the definition of a "payment stablecoin." However, issuers of arcade tokens often control the supply to dampen price increases (similar to airlines keeping the value of airline miles relatively stable over periods of time) and sometimes offer redemption rights (similar to credit card companies offering to redeem rewards points or offer cash back rewards).

As a result, the Proposed Rule's broad definition of "payment stablecoin" could create confusion regarding the permissibility of arcade tokens. Ultimately, the fact that loyalty and rewards points like airline miles are issued in tokenized form on a blockchain does not mean they should be classified as "payment stablecoins"—such assets do not require reserves,

[3] 12 U.S.C. § 5901(22)(A)(i).

[4] Miles Jennings, Scott Duke Kominers, & Eddy Lazzarin, *Defining tokens*, a16z crypto (Mar. 5, 2025), https://a16zcrypto.com/posts/article/defining-tokens/.

and the expectations of consumers are fundamentally different as compared to stablecoins. Notably, arcade tokens also do not pose the consumer protection, liquidity, illicit finance, or systemic risks that GENIUS was intended to address; rather, they enable activity within discrete, self-contained networks that utilize their own digital economies. Accordingly, the final rule should clarify that arcade tokens fall outside the scope of the definition of "payment stablecoin" under the proposed rule.

C. The Final Rule Should Clarify the Definitions of "Lawful Order" (Question 7) and "Account."

Treasury appropriately asks whether its description of "lawful order" is sufficiently clear. The question is important, both for government agencies and courts (both of whom will issue the lawful orders) and the companies themselves (who are required to comply with them). And clarity is especially important here, given the context in which such lawful orders are deployed: to seize, freeze, burn, or stop the transfer of payment stablecoins. While PPSIs will certainly try to abide by the terms of such orders, given the time sensitivities (often the orders involve exigent circumstances), the underlying subject matters (potential sanctions evasion or other illicit transactions), and possible third-party interests, it is important to ensure that the terms are clear and administrable.

The proposed rule defines "lawful order" as: "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: (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."[5]

First, the definition of "lawful order" should be clarified to allow parties to fully exercise their rights on available appeals before action by the PPSI is required. In other words, "final" should effectively mean "final after appeal." Currently, the proposed rule defines "lawful order" as "any final and valid writ, process, order, rule, decree, command, or other requirement issued or promulgated under Federal law." The definition potentially poses a problem where the agency issuing the order views its order as "final," but the order is appealable.

[5] *See* 12 U.S.C. § 5901(16).

For example, in the event OFAC demanded a PPSI to freeze a third-party's stablecoins or if a PPSI received a seizure warrant from a law enforcement agency, either the PPSI or a third party might seek judicial review of that order or warrant. It is unclear, however, whether the order/warrant becomes "final" for purposes of the Proposed Rule. If it is "final" but also subject to appeal, then the PPSI has a difficult choice. Similarly, if the third-party sought relief in court, under the current definition, it would seem the PPSI might have to act in accordance with OFAC's order in the face of significant liability if the third-party is ultimately successful. Therefore, the final rule should redefine "final" as "a decision or judgment that is not subject to further appeal, either because no appeal is available, the time for appeal has expired, or any appeal taken has been fully resolved, by the PPSI or any interested third-party." And providing a consistent, clear definition of "final" ensures that both the government and complying PPSIs understand their obligations.[6]

Moreover, the final rule should further define "account" to ensure (1) it is sufficiently clear to those required to comply with the "lawful order" what compliance entails; and (2) that complying with the "lawful order" is technically feasible. Importantly, a definition that is overly broad could make compliance unreasonable if not wholly impossible. For example, an order from law enforcement to "freeze all tokens related to person X" mistakenly assumes that a PPSI would have such information to connect the tokens to a given person. Such a definition could frustrate innovation in the stablecoin space, materially invite harm and loss to innocent third parties, and undermine the effectiveness of the compliance program the rule intends.

Further, it is fundamentally inequitable to impose requirements on PPSIs that cannot be met in practice. To clarify the meaning of "account," and thus a PPSI's compliance obligations under a "lawful order," the definition should expressly include one or more wallet addresses.[7] This revision carries several advantages: it is currently the approach that many law enforcement agencies use, such as the FBI and IRS-CI, to issue their orders and inquiries to industry. Moreover, such an approach minimizes harm to innocent third parties that would clearly occur without wallet-specific identification and instructions.

Alternatively, given the substantial liability PPSIs could face simply by acting in good faith in accordance with a "lawful order," the final rule

[6] For instance, under the Administrative Procedure Act, typically only "final agency actions" may be appealed for judicial review. *See* 5 U.S.C. § 704.

[7] Similarly, the definition of "lawful order" in proposed section 1010.100(rrr)(2) should make clear that, rather than having the order "specif[y] the payment stablecoins or accounts," such orders should "specif[y] the payment stablecoin wallet address" whenever possible.

could require that a "lawful order" would be one that sufficiently protects the PPSI from third-party claims. The situation is not difficult to imagine: a PPSI receives a seizure warrant or some other order, requiring that it freeze certain tokens. Upon obeying the order, it may be subject to lawsuits from third parties–payees, joint accountholders, or the initial holder of the tokens–who may have an interest in such tokens. Indeed, even the threat of litigation, or the expense of having to appeal or analyze multiple freeze/burn orders, creates a significant risk and burden upon a PPSI for attempting to comply in good faith with law enforcement demands.

It is unlikely that Treasury can directly create some "safe harbor" from such third-party claims by regulation; such immunities can only be created by statute. However, the proposed regulations can create a *de facto* protection by ensuring that an agency "lawful order" must agree to indemnify the PPSI against claims by third-parties for monetary losses or other penalties arising out of good faith actions in compliance with "lawful orders." Indeed, in other contexts, the U.S. Government has agreed to indemnify private parties for acting in accordance with governmental requirements. For example, in government procurement law, government contracts can include indemnification clauses limiting the liability of contractors for certain losses against third-party claims and property losses.[8] A similar indemnification framework would foster an environment where PPSIs could continue to innovate while incentivizing them to comply fully with "lawful orders," without risk of expensive third-party liability.

IV. Combatting Illicit Finance in Secondary Markets

A. The proposed rule correctly proposes that PPSIs should not be deemed MSBs (Question 4).

The proposed rule correctly excludes PPSIs from the definition of "money services business." However, there may still be ambiguity around whether a PPSI issuing payment stablecoins as well as engaging in activities that would be traditionally reserved to "money services businesses" might need to comply with both requirements for "money services businesses" under 31 CFR § 1022 and PPSIs under 31 CFR § 1033. We are concerned that without an express carveout for all activities conducted by PPSIs, PPSIs may still be subject to the requirements imposed on "money service businesses," requiring two distinct compliance programs, training curriculums, varying SAR thresholds, and more. Therefore, the final rule should make clear that all activities conducted by a PPSI are affirmatively carved out from the definition of "money service businesses" so that PPSIs can operate under a single set of rules.

[8] 50 U.S.C. § 1431–1435.

This approach would be consistent with other entities that simultaneously qualify as two types of financial institutions. For instance, although a bank performs certain MSB activity (such as transfer of funds), banks and foreign banks are excluded from the definition of "money services business" in the BSA regulations.[9] The same is true for persons and entities registered with the SEC or CFTC, and their foreign equivalents.[10] Treasury has made clear that casinos–which often perform certain MSB activities (such as foreign exchange, check cashing, and wire transfers)–should be regulated only as casinos, rather than under two sets of rules.[11]

The "single financial institution" approach makes sense for both regulatory and logical reasons. As a regulated entity, a PPSI would be responsible for overseeing and assessing its risk; adjusting its rule sets and monetary thresholds; developing and implementing policies, procedures, and internal controls; training its staff; ensuring that it has a competent chief compliance officer to oversee day-to-day compliance; conducting independent testing on its AML program; and performing a host of other obligations. The best way to ensure that this can be performed is by having an enterprise-wide system to hug the shoreline of a single set of rules; the best way to invite failure and noncompliance is to require a company to navigate two sets of regulations.

The regulatory benefit extends to the government, as well. Because the government employs different sets of examiners depending upon the type of financial institution being examined,[12] having an entity subject to a consistent set of examination expectations and exam teams is both sensible and efficient, and therefore aligned with the Administration's priorities to streamline regulatory compliance obligations.

---

[9] 31 CFR § 1010.100(ff)(8)(i).

[10] *Id.*

[11] Financial Crimes Enforcement Network, FinCEN Ruling 2005-5 (July 6, 2005), Definition of Money Services Business (Casinos as Money Services Businesses), https://www.fincen.gov/system/files/administrative_ruling/fincen_ruling2005-5.pdf.

[12] FinCEN has delegated its examination functions to a variety of regulators. For instance, banks are typically examined by their prudential regulators (such as the Office of the Comptroller of the Currency, the Federal Reserve, or the Federal Deposit Insurance Corporation). *See* 31 C.F.R. § 1010.810(b)(1)-(3). Brokers and dealers in securities are examined by the SEC. *See* 31 C.F.R. § 1010.810(b)(6). Certain non-bank financial institutions, such as MSBs, casinos, and precious metals dealers, are examined for BSA/AML compliance by the Internal Revenue Service. *See* 31 C.F.R. § 1010.810(b)(8). The GENIUS Act provides that PPSIs will be examined by their relevant primary Federal payment stablecoin regulator. 12 U.S.C. § 5905(a)(3).

B. FinCEN and OFAC Should Clarify that BSA Obligations Apply to Issuers Only at the Time of Payment Stablecoin Issuance and Do Not Extend to the Issuer for Transactional Activity Occurring in the Secondary Market.

The proposed rule obliges PPSIs to possess "the technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations . . . [for] transactions by third parties, including where a transaction results in an interaction with a permitted payment stablecoin issuer's smart contract." While these technical capabilities are critical to ensuring that PPSIs can comply with lawful orders, requiring PPSIs to use them to satisfy BSA and sanctions obligations in secondary markets is both unwise policy and, in many cases, impractical or impossible to implement from a compliance perspective. The requirement is also antithetical to the President's recently issued Executive Order, *Integrating Financial Technology Innovation Into Regulatory Frameworks*, which directs various federal agencies to review existing regulations to remove overly burdensome regulations and supervisory practices that hinder innovation in the financial technology sector.[13] And it runs afoul of the Administration's "whole of government" approach to further innovation and ensure that U.S. companies are not unfairly prejudiced in the marketplace. The final rule should revisit a PPSI's responsibility in the secondary market where they lack meaningful visibility, and establish a tailored approach that is reasonable and feasible for PPSIs to implement.

As FinCEN correctly proposes, PPSIs "should not be required to monitor secondary market activity," but instead should "be required to understand the risk its customers pose as part of its due diligence, as well as its distribution channels." FinCEN further identifies that PPSI responsibilities should be limited to those entities that have direct contractual obligations with the PPSI. This is eminently sensible, and consistent with Treasury's general approach to illicit finance compliance expectations and the fair limitations upon accountability.[14] OFAC's proposed rule should follow the same principle: the sanctions rules should only impose requirements on PPSIs for transactions where there is a direct contractual relationship between the PPSI and its "customer." Similarly,

---

[13] Exec. Order No. 14405, I*ntegrating Financial Technology Innovation Into Regulatory Frameworks*, 91 Fed. Reg. 30475 (May 19, 2026), https://www.whitehouse.gov/presidential-actions/2026/05/integrating-financial-technology-innovation-into-regulatory-frameworks/.

[14] Indeed, there is no general expectation for a financial institution to know the particulars of a company's "customer's customer." *See, e.g.,* Financial Crimes Enforcement Network, FIN-2020-G002, *Frequently Asked Questions Regarding Customer Due Diligence (CDD) Requirements for Covered Financial Institutions* (Aug. 3, 2020), https://www.fincen.gov/system/files/2020-08/FinCEN_Guidance_CDD_508_FINAL.pdf.

OFAC requirements should be limited to compliance programs that allow PPSIs to mitigate the "risk[s] its customers pose."

In addition, the final rule should further define "customer" to reflect that only those entities that have a direct contractual relationship with the PPSI, i.e. "a person that purchases (through any consideration) the products or services of a PPSI directly from the PPSI." Clarifying that "customer" is limited to direct customers of the issuer would appropriately tailor PPSI obligations. The final rule should make explicit that both FinCEN and OFAC requirements are limited to due diligence of "customers."

Importantly, the existence of a smart contract provides very limited visibility, providing only rudimentary information related to the third-party, most notably the third-party's wallet address. A PPSI is not privy to information identifying the third-party's name, geographical location, or business operations. The wallet address is insufficient for PPSIs to police the secondary market for comprehensive compliance with all OFAC requirements. Indeed, identifying transactions with "shadow" SDNs, non-SDN persons residing in sanctioned jurisdictions, specific sectorally-focused restrictions, and much more, could be very difficult, and in some cases impossible, for PPSIs depending on the specific technical limitations inherent in the design of a smart contract. Thus, a strict requirement to monitor secondary market transactions would be operationally impractical and greatly hinder stablecoin use and adoption.

At the very most, for secondary market transactions, the final rule could require PPSIs to incorporate technical capabilities that would allow them to screen the wallet address against the relevant designated wallets as specifically identified and published by OFAC. As noted above, a smart contract might be able to identify a specific wallet address, allowing it to prohibit a transaction with such address. Indeed, it is helpful that OFAC publishes such sanctioned wallet addresses, giving clear direction for screening and blocking.

Much of the challenge comes from the suggestion in the Proposed Rule that in the secondary market – after the PPSI has issued the stablecoins to its customer – it still "*exercise[s] possession or control of such stablecoins, including through smart contracts*."[15] This predicate is incorrect. Creation and operation of a smart contract does not establish ongoing control, and the PPSI no longer has possession of the stablecoins. At bottom, different PPSIs and different companies may be able to address these obligations in different ways. We recommend that whatever rules

[15] *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements*, 91 Fed. Reg. 18582, 18605 (Dep't Treasury Apr. 10, 2026).

apply, they should be technology-agnostic and not effectively or inadvertently ban certain technology over others or drive it offshore.

We fully agree with Treasury that the United States has critical national security, law enforcement, and economic interests in ensuring that the U.S.-based stablecoin ecosystem thrives and is successfully deployed across the globe. Thus, imposing expectations to surveil, assess, and affect (by blocking, freezing, or otherwise impacting) transactions in the secondary market long after issuance must be realistic and practical. This is especially true where PPSIs may be subject to strict liability for violations, and where there is the threat of criminal exposure and individual liability for officers, directors, and employees. Indeed, OFAC has an institutional interest in the global proliferation of USD-backed stablecoins because sanctions authority ultimately depends on visibility and jurisdictional leverage tied to USD-denominated financial flows. Without U.S. leadership in the stablecoin space, others, including China, will move to fill the technological void. If cross-border digital transactions migrate to instruments beyond U.S. control, OFAC's ability to monitor financial flows, enforce reporting and blocking requirements, and enforce its rules will be more difficult.

C. The OFAC Sanctions Compliance Program (SCP) Rule

The Proposed Rule imposes a novel regime upon PPSIs – namely, the obligation for PPSIs to maintain an appropriate, risk-based sanctions compliance program. To be clear, a16z fully appreciates that the sanctions program requirement comes from the GENIUS Act statutory provisions themselves, not from the Proposed Rulemaking. Nevertheless, there are a number of concerns with the Proposed Rule, which go well beyond the directions of Congress and would be inappropriate to impose on PPSIs.

Title 12 U.S.C. § 5903(a)(5)(A)(vi) provides that PPSIs be deemed "financial institutions" under the Bank Secrecy Act, "and as such, shall be subject to all Federal laws applicable to a financial institution located in the United States relating to economic sanctions, prevention of money laundering, customer identification, and due diligence, including – … (vi) maintenance of an effective economic sanctions compliance program, including verification of sanctions lists, consistent with Federal law."

Despite the predicate in Subsection 5903(a)(5)(A), the Bank Secrecy Act does not require the existence or maintenance of any OFAC compliance program for other "financial institutions." And while the existing sanctions laws – such as TWEA, IEEPA, and the Kingpin Act – establish sanctions programs and prohibit violations, those laws (and OFAC implementing regulations) contain no requirement for financial institutions or other entities to actually maintain a compliance program.

The preamble to the proposed Rule points to its previous guidance, and notes that OFAC settlement agreements "usually insist upon an implementation of a sanctions compliance program in line with the 2019 Compliance Framework."[16] Three points are notable: first, the guidance to which OFAC points indicates that a sanctions compliance program is encouraged, but not required. And even OFAC's *Introduction to the Office of Foreign Assets Control*, published just last week, specifies that these compliance programs are "encourage[d]" and should not be a "'one-size-fits-all' compliance program suitable for every organization" or spelled out to the prescriptive detail in the Proposed Rule.[17] Second, those compliance programs were a function of post-enforcement settlements with companies that had already been found to have violated the sanctions laws, often repeatedly and often with accompanying egregious circumstances surrounding the violations. And third, none of those agreed-upon compliance programs made as a condition of settlement were as extensive as what exists in the Proposed Rule. In other words, the Proposed Rule is more demanding upon PPSIs who have done nothing wrong than the consent orders are against companies who have been found to have actually violated the law.

So, while Subsection 5903(a)(5)(B) requires Treasury to promulgate regulations, "tailored to the size and complexity of permitted payment stablecoin issuers," nothing in the GENIUS Act suggests that Congress anticipated that OFAC would design such an extensive, overbroad regime to be imposed on this burgeoning industry. Rather, the legislative direction requires only the following: first, that the compliance program be "effective"; that it includes "verification of sanctions lists"; and that the proposed regulations be "tailored to the size and complexity" of the PPSIs. 12 U.S.C. § 5903(5)(A), (B).

As proposed, the Sanctions Compliance Program (SCP) rules go far beyond Congress' direction. They also provide for unmanageable, and sometimes impossible, regulatory expectations, which make them decidedly "ineffective." For instance, Proposed 502.201(b)(2)(i) insists that the PPSI conduct a holistic risk assessment that considers not only counterparties, but also "*indirect* points of contact with foreign persons or persons residing in foreign jurisdictions." Potentially, this would mean that a PPSI would need to assess whether, years after the initial issuance of a certain stablecoin, the PPSI's "customer's customer" has such risk, or whether a transferee a hundred transactions away was somehow a foreign person, or resident in a foreign jurisdiction. Regardless of technology, there

[16] *Id.* at 18614.

[17] Office of Foreign Assets Control, *Introduction to the Office of Foreign Assets Control* (June 1, 2026) at 7, https://ofac.treasury.gov/media/935656/download?inline.

is no meaningful way to assess whether any company could ever perform such a task or competently assess such risk.

Similarly, in the subsection on Internal Controls (91 Fed. Reg. 18660), Proposed Section 502.201(b)(3), the Proposed Rule requires that the PPSI must establish internal controls, including technical controls, "applicable to all payment stablecoin-related activity, *whether on the primary or secondary market*" despite the fact that a PPSI will have limited visibility into such secondary markets. Even if one could find more visibility into these markets (perhaps by blockchain analytics, open source research, or other information), in many instances there may be no realistic way for the PPSI – the original issuer – to control certain secondary market activity, regardless of whether it is included in a PPSI's sanctions compliance policy or other program document.

As noted above, the GENIUS Act language provides that the rule for an SCP has three characteristics: (1) it should be effective; (2) it should include "verification of sanctions lists"; and it should be "tailored to the size and complexity of permitted payment stablecoin issuers." As drafted, the Proposed Rule is not tailored to the size, complexity, or even the capability of PPSIs, and the rule contains no mention of sanctions screening lists.

Finally, we appreciate Treasury's question[18] regarding the suggested implementation timeline for the SCP to go into effect. While many existing stablecoin issuers already perform robust sanctions screening, they have never been subject to an express regulatory requirement to do so. And, in fact, no financial institution or company has been subject to an SCP rule, so there are no models upon which to build, modify, or extrapolate. Thus, there are few examples, third-party compliance providers, or technology solutions to help companies meet the specific regulatory directives once these rules are made final. Therefore, we respectfully recommend that Treasury should provide for a two-year implementation deadline for PPSIs to come into compliance with the rule once finalized.

D. The Final Rule Should Concretely Authorize the Use of Innovative Technologies to Meet BSA and OFAC obligations.

Section 9 of the GENIUS Act reflects Congress's intent to promote innovation in detecting illicit activity, like money laundering. Specifically, Section 9 states that Treasury "shall seek public comment to identify innovative or novel methods, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit

[18] *Permitted Payment Stablecoin Issuer Rule*, 91 Fed. Reg. at 18620.

activity, such as money laundering, including digital assets."[19] The Act also requires FinCEN to "issue public guidance and notice and comment rulemaking . . . relating to . . . [t]he implementation of innovative or novel methods, techniques, or strategies by regulated financial institutions to detect illicit activity involving digital assets," among other things.

The Final Rule should affirmatively endorse the use of innovative technologies to combat illicit finance. Indeed, technologies like digital identity and artificial intelligence offer substantial promise for detecting, identifying, and preventing illicit finance, including money laundering and sanctions evasion. Artificial intelligence, in particular, can be deployed in various ways to fight illicit finance including enhanced AML detection, the implementation of effective internal controls, and streamlining reporting.[20] We believe that AI-enabled tools are the most practical path for financial institutions such as PPSIs to build effective AML/CFT and sanctions programs at scale. They are particularly well-suited to diligence-driven compliance tasks, such as sanctions screening, beneficial ownership review, adverse media review, financial analysis, and customer risk scoring. As PPSIs create new AML/CFT programs ahead of full GENIUS Act implementation, AI tools offer the most efficient way to build those programs effectively and at a lower cost than legacy compliance tech. However, the primary barrier to adopting innovative approaches, including AI and other advanced compliance tools, is not the technology itself but regulatory uncertainty. That uncertainty slows technology adoption and pushes institutions to rely on outdated systems that are demonstrably less effective at identifying illicit activity.

This Final Rule presents an opportunity to address that barrier. FinCEN states that its Proposed Rule is designed to "encourage instances where a PPSI finds it beneficial to consider and evaluate technological innovation and, as warranted by the PPSI's risk profile, implement new technology or innovative approaches in combating financial crime."[21] The

---

[19] GENIUS Act § 9.

[20] To that end, Treasury (along with the banking regulators) should revise or wholly rescind their *Joint Statement*. *See* Board of Governors of the Federal Reserve System et al., *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf. While we applaud the government's efforts to encourage innovative efforts, the document opens the door to pilot programs, but without any means or timeframe as to when to stop running their original programs in parallel. As a result, covered entities are left with little incentive to actually consider innovative efforts, and run the risk of being expected to run duplicative, expensive dual programs even after their innovations might prove more effective.

[21] *Permitted Payment Stablecoin Issuer Rule*, 91 Fed. Reg. at 18636. Similarly, Section 6002(3) of the Anti-Money Laundering Act of 2020, Pub. L. 116-283, 134 Stat. 4549, states that among the purposes of the statute is to "encourage technological innovation and the adoption of

Proposed Rule itself (at Section 1033.221) would require FinCEN, before an enforcement action or significant supervisory action, to consider the extent to which the PPSI has conducted "innovative technologies producing demonstrable outputs" evincing the effectiveness of the AML program, including the "effective use of artificial intelligence, federated learning, and other advanced monitoring tools."[22] Another proposed rule from FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism Programs,"[23] identifies "machine learning, generative artificial intelligence (GenAI), digital identity, blockchain monitoring and analytics, or application programming interfaces (APIs)"[24] as relevant innovative approaches, and, most importantly, provides that institutions that *"responsibly experiment with innovative technologies in their AML/CFT programs will not incur any additional risk of being subject to a significant supervisory AML/CFT action or AML/CFT enforcement action solely based on the use of innovative technologies."*[25] a16z strongly supports each of these.

This protection, however, is meaningful only if it is paired with the broader supervisory and enforcement reforms other Proposed Rules contemplate for banks.[26] As long as examiner findings can accumulate around an institution's use of innovative technology through informal supervisory channels that fall below the threshold for FinCEN consultation, the formal protection against "significant" supervisory action will offer institutions limited practical comfort. The protection for innovative technology and the strengthening of the notice and consultation framework are therefore inseparable: each is necessary to give the other meaningful effect.

Furthermore, we respectfully request that FinCEN confirm that responsible implementation and experimentation of new technology includes the freedom to pilot, test, refine, and even discontinue AI tools and digital identity techniques without supervisory penalty. Innovation by definition involves iteration. Supervisory expectations should accommodate the trial-and-error inherent in deploying new technology, including periods when a new tool is being calibrated or run in parallel with legacy systems.

---

new technology by financial institutions to more effectively counter money laundering and financing of terrorism."

[22] *Permitted Payment Stablecoin Issuer Rule*, 91 Fed. Reg. at 18665.

[23] *Anti-Money Laundering and Countering the Financing of Terrorism Programs*, 91 Fed. Reg. 18704 (Dep't Treasury Apr. 10, 2026).

[24] *Id.* at 18712.

[25] *Id.*

[26] *See id.* at 18304.

Moreover, to drive adoption of innovative technology by PPSIs, FinCEN must pair these reforms with affirmative, specific guidance. This includes examples of technologies FinCEN recognizes as covered under innovative technology protections, and assurance that examiners will apply the framework fairly and objectively even when they are unfamiliar with the tech. As we have noted in our prior comment letter to Treasury on innovative methods to detect illicit activity involving digital assets,[27] earlier interagency efforts have encouraged innovation in principle but, in practice, left financial institutions without the signals or assurances they need to determine whether their efforts will be acceptable to regulators.

Specific guidance and meaningful safe harbors for the use of innovative technology, including AI tools and digital identity methods, are necessary. As drafted, the pending proposed rule on this topic provides little incentive for an institution to pilot or implement innovative technology that carries the risk of supervisory uncertainty and heightened scrutiny. Legacy tools that examiners are already familiar with carry the advantage of regulatory familiarity, even when they are materially less effective at identifying illicit activity. Incentives matter: institutions will invest in new technology only when they rationally believe that their investment will be acceptable to regulators.[28] Without explicit direction and protections from FinCEN, the rational choice for many institutions will be to forgo these innovative tools, even where they would meaningfully reduce compliance cost and improve the detection and prevention of ML/TF.

Accordingly, we urge FinCEN to take two actions to give the protection for innovative technology operational effect. First, FinCEN should publish non-exhaustive, illustrative examples of specific use cases that fall within the innovative technology protections. These could include, for instance, AI-enabled sanctions screening; machine-learning-based transaction monitoring; digital-identity-based customer identification and verification; blockchain analytics for source-of-funds and beneficial ownership analysis; generative AI for drafting SAR narratives and other compliance documentation; AI-assisted customer due diligence and adverse-media screening; and API-based information sharing between institutions. Publishing illustrative examples would give institutions a clear understanding of what categories of innovative technology are protected by

[27] *See* Letter from Miles Jennings, Michele R. Korver & Jai Ramaswamy, Andreessen Horowitz, to Julie Lascar, U.S. Dep't of the Treasury, *Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets,* (Oct. 17, 2025) at 7 (observing that the 2018 Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing "neither inspired nor incentivized" innovative approaches to compliance and that institutions will not invest in innovation absent "some clear and concrete signal that they will in fact be acceptable to regulators").

[28] *Id.* at 7–8 (observing that institutions will only invest in innovative compliance solutions when they "rationally believe that their investments in innovation will be worth it.").

FinCEN, while leaving room for new technologies to come within that protection as they emerge.

Second, FinCEN's guidance on innovative technology should be calibrated to PPSIs of different types, sizes, and stages, and be applied by examiners objectively, fairly, and consistently. What it means to "*responsibly experiment with innovative technologies*"[29] should reflect the institution's actual risk profile, resources, and operational realities rather than a single uniform expectation. The framework should also provide explicit protection against inconsistent examiner application and give institutions a clear escalation path when an examiner's treatment of an innovative tool departs from FinCEN's published guidance. Without protections of this kind, the risk of subjective or uncertain examiner review will continue to deter institutions from investing in the very technologies Treasury seeks to encourage.

E. The Proposed Rule Should Account for Critical User Privacy Concerns; and FinCEN should Revisit and Rescind its Pending Mixing Proposal.

One particular area of innovation and development that demands special attention is technology that allows users to retain their privacy. Today, most stablecoins run on open blockchains where every transaction—including amounts, counterparties, and frequency of transactions—is permanently and publicly visible.[30] Although many blockchain transactions are pseudonymous—meaning they do not have personally identifiable information associated with them on the blockchain—once a person's name is connected to a single onchain transaction, it is often possible to reconstruct that person's entire transaction history, particularly when using advanced blockchain analytics.[31]

---

[29] *Anti-Money Laundering Programs*, 91 Fed. Reg. at 18712.

[30] *See* Jai Ramaswamy et al., *a16z Letter to the Financial Crimes Enforcement Network: Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, a16z crypto*, (Jan. 22, 2024) at 5, https://dwt2zme5yrom6.cloudfront.net/uploads/2024/01/a16z-CVC-Mixing-Comment-filed.pdf. Separately but relatedly, we note that FinCEN has not yet acted upon its proposed "Mixer 311 Rule," initially proposed in 2023. *See Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, 88 Fed. Reg. 72701 (Dep't Treasury Oct. 23, 2023). Although the proposed rule has not gone into effect, so there is no attaching legal obligation, there is nevertheless an important effect, both factually and legally. In announcing the proposed rule, Treasury has made a series of erroneous factual determinations. As covered in more detail below, a16z respectfully suggests that this proposal, and especially the predicate factual findings, be rescinded for the reasons we have previously raised.

[31] Blockchain analytics can trace transactions back to a real-world user, despite the user's attempts to protect their identity. Thus, as characterized by one court, cryptocurrency

The concern is not hypothetical. The advantage of blockchain-predicated systems is that (for public blockchains), every transaction is traceable, allowing law enforcement and the intelligence community–and the public–visibility into transaction flows. But this comes at a cost for legitimate users who seek to use stablecoins and other digital assets for legitimate, everyday uses. Indeed, in some circumstances this technology is also essential to prevent harm. It allows people to make sensitive transactions, such as paying for healthcare services, in confidence.[32] It allows them to exercise their constitutionally protected associational rights.[33] It allows them to undertake activities that could draw retaliation from authoritarian regimes or foreign terrorists, such as donations to Ukrainians to fight against Russian invasion.[34] And it allows large holders of digital assets to keep their families safe by preventing others from discovering their holdings.[35] All of these activities are lawful, but all of them depend on privacy-preserving technologies like those targeted by the mixing rule.[36] Nearly everyone wants a basic degree of privacy for their lawful activity. In the traditional-finance world, participants rely on privacy-preserving technology like password-protected accounts and encryption-protected communications because it is irresponsible to expose all affairs to the public.[37]

To offer stronger consumer-data protections and meet other regulatory requirements, some blockchains adopt privacy-preserving tools that allow users to cryptographically reveal transaction data to specific parties such as regulators and auditors without full public exposure on the ledger. A zero-knowledge proof (ZKP) is but one example of this kind of

---

transactions are "both uniquely anonymous and uniquely public." *United States v. Sterlingov*, 2024 WL 860983, at *1 (D.D.C. Feb. 29, 2024).

[32] *See* Tuminelli & Whitehouse-Levine, *When Did Privacy Become a Bad Word?*, CoinDesk (Aug. 25, 2023), perma.cc/26PB-ZREX.

[33] *See* O'Sullivan, *What are mixers and "privacy coins"?*, Coin Center (July 7, 2020), perma.cc/J4G3-W9TQ.

[34] *See Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, CISA (May 9, 2022), perma.cc/C5TN-QL62.

[35] Kurt Robson, *$11M Crypto Gunman Targets Sam Altman-Linked Victim: How a Fake Delivery Driver Violently Stole Bitcoin And Ethereum*, Yahoo News (Nov. 26, 2025), https://www.yahoo.com/news/articles/11m-crypto-gunman-targets-sam-100215987.html (quoting the chief executive of a security firm who stated, "There's definitely an uptick in kidnappings targeting crypto owners.").

[36] *See* Weinstein, *AI and Blockchain Analytics: The Urgent Need for Crypto Privacy Tools*, Forbes (Apr. 7, 2023), perma.cc/M65D-4ER2.

[37] Of note, the importance of financial privacy is not a novel concept in the U.S. For instance, the Right to Financial Privacy Act of 1978 (RFPA) protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. *See* 12 U.S.C. §§ 3401–3423.

privacy tool. The final rule should note that use of privacy-preserving technologies, such as ZKPs, are a way to ensure the security and confidentiality of users for their legitimate purposes.[38]

But, FinCEN should go one step further and rescind or significantly revise its pending *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern* ("the mixing rule").[39] In addition to stifling innovation and advances in blockchain technology, the Proposal as written would substantially limit PPSIs' ability to use privacy-preserving technologies. We believe that privacy-preserving technologies, which this mixing rule targets, go hand-in-hand with legitimate and innovative uses of digital assets. Privacy tech is necessary for stablecoins to thrive, particularly for their use in everyday activities such as payments and settlement, and the mixing rule could significantly limit privacy protection options for PPSIs.[40]

As discussed in our response to the mixing rule proposal, FinCEN's stated premise that privacy-preserving technologies "undermin[e] the legitimate and innovative uses of CVC" is mistaken. While illicit conduct can thrive in a wide range of environments, many lawful activities require the security and confidentiality that only privacy-preserving technologies can provide. The history of the Internet provides a close analogy.[41] In the early days of the Internet, many believed that because of its anonymized, decentralized nature, it would be used primarily for crime and lawlessness.[42] Many held the view that the "internet cannot be regulated."[43] At the same

---

[38] The GENIUS Act itself raises privacy issues in connection with illicit finance regulation. For example, Section 9(b)(2)(D) requires FinCEN to consider privacy risks associated with the information that is collected or reviewed in connection with Treasury's research on the innovative "methods, techniques, or strategies" to address illicit finance.

[39] *Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern*, 88 Fed. Reg. 72701 (Dep't Treasury Oct. 23, 2023).

[40] *See e.g.*, *Implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act for the Issuance of Stablecoins by Entities Subject to the Office of the Comptroller of the Currency*, 91 Fed. Reg. 10202, 10292 (Mar. 2, 2026) (OCC proposed rule, proposed to be codified at 12 C.F.R. § 15.13(b)(4), which requires that a PPSI's "information technology and security program must include . . . safeguards designed to: (i) Ensure the security and confidentiality of records containing nonpublic personal information about a customer").

[41] *See* Sina Kian, *A Letter to the White House: Aleo's Response to the OSTP*, Aleo (Mar. 3, 2023), perma.cc/GSD3-5PLN.

[42] Goldsmith & Wu, *Who Controls the Internet* xii (2006) ("In the 1990s, many believed that nations could not control the local effects of unwanted Internet communications that originated outside their borders, and thus could not enforce national laws related to speech, crime, copyright, and much more").

[43] *Id.* (quoting MIT Media Lab co-founder).

time, law-abiding businesses and citizens did not rely on the Internet because their activities were too exposed and insecure without strong privacy guarantees. Then, a wave of privacy-preserving technologies, including some of the same encryption methods underlying modern blockchain technology, were introduced.[44] Instead of making the Internet home to *more* criminal activities, these technologies made it finally welcoming to lawful and institutional uses. Privacy-preserving technologies allow confidential information to be transmitted over the Internet securely and privately. As a result, hundreds of millions of Americans, as well as every major corporation and governmental agency, adopted the Internet for their most confidential activities, including their bank accounts, medical records, and personal communications. Thus, by the numbers, criminality became a smaller proportion of online activity. Today, privacy coexists with law-enforcement tools that allow meaningful investigation of activity on the Internet, including through technologies that have developed in tandem with the Internet and allow law enforcement to monitor and prohibit illegal activity without eliminating a basic level of privacy. If these privacy-preserving technologies had been stopped in their tracks, the Internet would have remained a wild west for people willing to take their chances with unprotected information. We would have never seen the ubiquitous lawful and institutional uses familiar today. The mixing rule as currently written risks realization of stablecoins' and the GENIUS Act's same potential.

Of utmost importance, the six categories of "mixing" defined by the proposed special measure reaches too much lawful activity. Although the proposal focuses on the illicit conduct that its six categories cover, their terms are very broad and appear to also reach routine and innocuous transactions. On our reading, they could reach basic practices like Unspent Transaction Output (UTXO)[45] transactions on certain blockchains, ordinary tools like smart contracts, as well as privacy-preserving technologies designed to protect stablecoin users' financial activities.

In addition, we believe that the mixing rule cannot be reconciled with the applicable statutory factors. Under Section 311 of the Patriot Act, FinCEN must balance how much the classified transactions are "used for legitimate business purposes" with how much they are "used to facilitate or promote money laundering in or through the [foreign] jurisdiction."[46] This statutory balancing requires FinCEN to recognize and account for the legitimate activities that its class of transactions encompasses. As such,

[44] *See, e.g.*, Singh, *The Code Book* 293–317 (1999).

[45] An Unspent Transaction Output or UTXO is an unused or leftover cryptocurrency in a transaction. Ledger Academy, *Unspent Transaction Output UTXO meaning* (July 23, 2023), perma.cc/Q2AQ-DQU2.

[46] 31 U.S.C. § 5318A(c)(2)(B).

FinCEN should take great care in designating a class of transactions as of primary money laundering concern where those transactions are overwhelmingly legitimate.[47] And, available data supports the exponential growth of stablecoin holdings and use.[48] We believe that FinCEN and OFAC can accomplish their AML/CFT goals without depriving stablecoin users of privacy in their financial lives. Few things have a higher place in American legal history than the "cherished privacy of law-abiding citizens."[49] "Privacy of personal matters is an interest in and of itself;"[50] it is protected by multiple provisions in our constitution;[51] it is protected by common law;[52] and it is guaranteed by numerous federal and state statutes.[53] We strongly urge FinCEN to rescind or narrow the proposed special measure to more appropriately balance PPSIs' use of emerging and privacy-preserving technologies with national security objectives.

F. Other Unintended Consequences of the Proposed Rule

Other components of the Proposed Rule are not necessarily problematic, but nonetheless warrant some comment and perhaps adjustment within the Proposed Rule. For instance, Proposed Section 1033.210(b)(1)(i)(B) requires PPSIs to review and incorporate into their risk assessments the AML/CFT Priorities as promulgated by FinCEN, as appropriate. This requirement parallels Treasury's similar proposal for other financial institutions, as reflected in its proposed revised AML Program Rule.[54]

While we have no objections to the general approach that a risk assessment should take into account government-wide priorities, we respectfully note two concerns. First, although the AML/CFT Priorities

---

[47] *See, e.g.*, Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitzlato, 88 Fed. Reg. 3919, 3924 (January 23, 2023): "The record further amply demonstrates that Biztlato's services are used, to an unusually large extent, to facilitate illicit finance, particularly when compared to other CVC exchanges.... [Bitzlato] has a high ratio of illicit transaction exposure relative to total transaction volume when compared to other exchanges, and it has served as the second largest attributable counterparty for the largest darknet market in the world and continues to support Russia-connected darknet markets."

[48] Daren Matsuoka et al., *State of Crypto 2025: The year crypto went mainstream*, a16z crypto (Oct. 22, 2025) at 18–20, https://perma.cc/NY7V-PLU4.

[49] *United States v. United States District Court*, 407 U.S. 297, 312 (1972).

[50] *Roberts v. Austin*, 632 F.2d 1202, 1214 (5th Cir. 1981).

[51] *E.g.*, *Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373 (2021); *Katz v. United States*, 389 U.S. 347 (1967); *Carpenter v. United States*, 585 U.S. 296 (2018).

[52] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[53] *See* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3423 (protecting the confidentiality of personal financial records).

[54] *Anti-Money Laundering Programs*, 91 Fed. Reg. 18704.

describe highlighted areas of concern, there is little guidance for many financial institutions–especially PPSIs–on how these priorities are relevant to the precise businesses. Second, FinCEN's AML/CFT Priorities were initially issued on June 30, 2021. Those Priorities, developed pursuant to Section 6101 of the Anti-Money Laundering Act of 2020, must be reissued every four years; therefore, they are now expired. We suggest that when Treasury revises and reissues the new set of AML/CFT Priorities, the rule deadlines should be extended accordingly to allow PPSIs to prepare and appropriately fashion their respective risk assessments.

Finally, we note that although the Proposed Rule would require that PPSIs collect beneficial ownership information regarding legal entity customers, FinCEN has not yet proposed a CIP Program rule for PPSIs. (91 Fed. Reg. 18604)

V. Conclusion

We are deeply committed to the development of a legal and regulatory framework for stablecoins and other crypto assets, which we believe is critical to fostering innovation while protecting market participants and the safety of the financial system. To that end, we hope that our observations and comments will be of assistance to FinCEN and OFAC. We greatly appreciate the opportunity to provide comments on these important matters, and we look forward to continued engagement with FinCEN and OFAC on these issues.

Respectfully submitted,

Miles Jennings, Head of Policy & General Counsel
a16z crypto

Michele R. Korver, Head of Regulatory
a16z crypto

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z