ANDREESSEN
HOROWITZ

August 21, 2026

BY ELECTRONIC SUBMISSION

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

Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Office of the Comptroller of the Currency
400 7th Street SW, Suite 1E-F216
Washington, DC 20219

National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: Request for Comment on Permitted Payment Stablecoin Issuer Customer Identification Program (FINCEN-2026-0101 / OCC-2026-0331 / RIN 1557-AF53)

Andreessen Horowitz ("a16z") appreciates the opportunity to respond to the Department of the Treasury's (the "Department" or "Treasury") request for comment, dated June 22, 2026, (the "Request"), on the joint proposed rule by the Financial Crimes Enforcement Network ("FinCEN"), the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA")[1] to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins ("GENIUS") Act.[2] The government has taken a thoughtful approach to implementing the GENIUS Act, and we are grateful for the Agencies and their respective staffs' commitment to soliciting information from the public through a transparent process in attempting to fashion an appropriate Customer Identification Program ("CIP") rule for permitted payment stablecoin issuers ("PPSIs").

[1] Collectively, FinCEN, the OCC, the Board of Governors of the Federal Reserve, the FDIC, and the NCUA will be referred to as "the Agencies."

[2] *Permitted Payment Stablecoin Issuer Customer Identification Program*, 91 Fed. Reg. 37234 (Dep't Treas. June 22, 2026) (the "Proposed Rule").

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. Our portfolio companies include stablecoin issuers, infrastructure providers, and custodians, and 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 and the integrity of the U.S. financial system. To that end, we hope that our observations, drawn from our deep experience, can be of assistance to the Agencies in drafting the Final Rule.

II. Executive Summary

In this comment to the Proposed Rule, we have focused upon specific issues where we believe we can provide the most useful insights. First, the Final Rule should maintain its focus upon primary market activity only. This would be consistent with the Agencies' approach for other financial institutions, and would align with the governing statutes, including both the Bank Secrecy Act ("BSA"), which requires CIPs for the primary conduct of opening an account, and the GENIUS Act, which requires identification programs for account holders with the PPSI, rather than further downstream accounts or subsequent (or previous) transactions. The focus on the primary market is also consistent with the realities of these markets.

Further, the regulatory definition of "account" should be refined and narrowed to ensure that the PPSI and the customer have a bilateral agreement and that the PPSI has onboarded the person for ongoing direct access for uses of the account. The Proposed Rule's current framework for "account" provides insufficient clarity as to what the relationship entails. This gap should be fully resolved in the Final Rule by not only narrowing the definition of account, but also further establishing what activity would not establish an account relationship. There should be clear exclusions to the definition of "account," beyond those already set forth in the proposed rule, to ensure that PPSIs are able to comply with the Final Rule once promulgated.

Next, a "walk-up redeemer" should not be considered an account relationship and should not require a CIP. For entities or individuals (other than an accountholder) seeking to redeem a stablecoin, there is no reason to onboard such single-use redeemers for account openings. The Final Rule should make clear that this kind of occasional redemption transaction does not fall within the scope of CIP expectations.

Crucially, the Final Rule should encourage and facilitate the use of digital identity verification methods. The Final Rule should keep CIP requirements flexible and technology-neutral, expressly permitting digital identity methods like state-issued mobile IDs, alongside non-governmental alternatives such as third-party identity networks, biometrics, decentralized identifiers, and verifiable credentials, since traditional document checks have grown impractical for remote institutions and expose customers to fraud. The Final Rule should also allow for privacy-preserving verification techniques like zero-knowledge proofs to satisfy verification and recordkeeping obligations, reducing unnecessary data exposure and cybersecurity risk. Importantly, the Final Rule should not add unnecessary and burdensome documentary capture requirements, as deepfake-driven fraud makes document collection an unreliable standalone protection.

The Final Rule should also permit a PPSI to rely upon another qualified PPSI's CIP for its own identity verification procedures. This would avoid the unnecessary and duplicative nature of one customer or entity verifying its identity multiple times with multiple different institutions. This kind of excessive divulgence of personally identifiable information (including name and address, among others) could subject customers to enhanced risks of theft and fraud by cybercriminals. Finally, the enterprise-wide CIP allowance should be expressly codified and provide explicit authorization for enterprise-wide CIP programs. While this is noted in the preamble of the Proposed Rule, we respectfully submit that the Final Rule includes this clarifying language so that institutions will be able to share such programs.

III. Comments in Response to the Agencies' Proposed Final Rule

A. The Final Rule Should Focus Only Upon Primary Market Activity

Request for Comment 1*: Should any CIP requirement be extended to secondary market activity? If yes, in what circumstances? What would be the benefits and drawbacks of doing so?*

No, the CIP requirements should cover only primary market activity. The Agencies appropriately focus the rule upon activity in connection with the primary market–that is, in connection with the PPSI's direct customers. This is consistent with the approach of CIP rules for other financial institutions, such as banks, brokers or dealers, mutual funds, futures commission merchants, and other institutions with a CIP program requirement.

This focus is instructed by the governing statutes themselves. The relevant provisions of the Bank Secrecy Act, 31 U.S.C. 5318(l)(1) authorize promulgation of a CIP rule to establish minimum standards "in connection with the opening of an account" (*i.e.*, not for secondary market transactions). In other words, the statutory predicate for the CIP regulations is for account onboarding only, not for downstream (or upstream users).

The text and structure of the GENIUS Act itself also corroborates this conclusion that the CIP rule must be directed only to primary markets. For example, it is possible that blocking, freezing, and rejection of transactions should extend to secondary market activity–only if and when feasible. But this is considered in an adjacent provision, 12 U.S.C. 5903(a)(5)(A)(iv), unlike the CIP statutory authority, which pertains to "*identification and verification of account holders with the permitted payment stablecoin issuer*" (emphasis added) *see* 12 U.S.C. 5903(a)(5)(A)(v). Had Congress intended the CIP regulations to extend beyond account holders, it would have written this subsection differently.

It is also consistent with the logic behind CIP programs generally: to ensure that the financial institution has a "reasonable belief" in the identity of its customer prior to account opening. *See*, *e.g.*, 31 C.F.R. 1020.220. The regulators have repeatedly stressed that CIP rules are an important part of an institution's BSA/AML program, but that it is designed for understanding one's direct counterparty, rather than downstream users.[3] In short, as the name implies, a "customer identification program" is directed for information regarding the customer, not subsequent (or previous) indirect customers-of-customers or users.

And finally, cabining CIP programs to primary market activity is sensible given the realities of the market to be regulated. The BSA itself notes that the CIP rule is designed to "verify the identity of any person seeking to open an account *to the extent reasonable and practicable.*" 31 U.S.C. 5318(l)(2)(a) (emphasis added). According to the Agencies' own Regulatory Impact Analysis, there are approximately 50 PPSIs, with an average of 1,000 primary market customers.[4] Performing CIP on these 1,000 customers is difficult in itself. Globally these numbers are in the hundreds of millions of users. In short, it is simply impossible to envision a situation in which any financial institution – bank, PPSI, or any other entity – would be able conduct CIP on such an entire collection that comprises the secondary market. Such a rule, if promulgated, would prove neither "reasonable" nor "practicable."

B. The Definition of "account" should be Refined and Narrowed

Request for Comment 2*: Should FinCEN and the Agencies refine or clarify its definitions of account, customer, or digital asset service provider? Are additional definitions needed?*

Request for Comment 3*: Should FinCEN and the Agencies retain "formal relationship" as part of the definition of account? What are the hallmarks of a "formal relationship" between a PPSI and a user? Should FinCEN and the Agencies provide examples or attributes of a formal*

---

[3] *See also*, *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act*, Financial Crimes Enforcement Network (April 28, 2005) https://www.fincen.gov/resources/statutes-regulations/guidance/interagency-interpretive-guidance-customer-identification.

[4] Proposed Rule at 37246 and 37248.

relationship in guidance? Would other concepts be a better foundation for the account definition, such as a contractual or business relationship, and why?

The definition of "account" in Section 1033.100(a) appropriately insists on a "formal relationship" between the PPSI and the customer.[5] Such an approach is consistent with the restriction above (that the CIP rule extends only to the primary market), and ensures that the regulatory expectation be extended to those not in privity. But as drafted, the Proposed Rule provides insufficient clarity as to what the relationship entails "to provide or engage in services, dealings, or other financial transactions," followed by a nonexhaustive list. Rather, the Final Rule should ensure that the PPSI and the customer (1) have entered a bilateral agreement (evinced through acceptance of a terms of service, or functional, contractual equivalent); and (2) the PPSI has onboarded the person for ongoing (rather than occasional or single-use) direct access for issuance, redemption, managing reserves, or custody.[6]

It is also critical to specify what activity would *not* establish an account relationship. To that end, there must be clear exclusions to the definition of "account" to ensure that PPSIs are able to comply with the Final Rule once promulgated. Proposed Rule 1033.100(a)(2) already includes certain exclusions; while those listed are appropriate, they are also incomplete. For instance, the rule should expressly indicate that certain kinds of activities – especially those activities taken for compliance reasons – should not be deemed to create a "formal relationship": (1) receipt of tokens resulting from a third-party transfer; (2) freezing/burning/seizing a stablecoin pursuant to a lawful order, or for any other compliance reason, including anti-fraud, consumer protection, anti-money laundering, or countering sanctions evasion; or (3) any equivalent activity that results in the issuance, redemption, management, purchase, sale, or providing custodial or safekeeping services for reasons connected to following a law, regulation, or lawful order.

C. A "Walk-Up Redeemer" Is Not an Account Relationship Requiring a CIP

Request for Comment 4: *Should the proposed rule be clarified or refined to account for situations where a customer's only desired relationship with a PPSI is to redeem a payment stablecoin?*

---

[5] Proposed Rule at 37239. *See also* FFIEC Manual, *Customer Identification Program*, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/01 (describing an "account" for CIP purposes as "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account, or other extension of credit.").

[6] The language at Proposed Rule 1033.100(a)(1)(iv), which would include "other activities that directly support activities" in (a)(1)(i)-(iii) would arguably reach vendors and other service providers, although those entities should clearly not be deemed "customers" under the CIP rule. As such, the language should probably read as "other activities that directly support activities *to the person*" who opens the account for the issuance, redemption, custody, *etc*. as part of the same formal relationship.

There will be situations where an entity or individual other than an accountholder seeks to redeem a stablecoin. Analogous to the redeemer of a cashier's check at a bank, there is no reason to onboard this single-use redeemer for account opening, and there is no basis for triggering the CIP rule. The Final Rule should thus make clear that occasional redemption transactions do not fall within the scope of CIP expectations.

To be sure, this exclusion does not mean that such occasional transactions by "walk-up" redeemers are invisible to anti-money laundering compliance. Rules such as the Funds Transfer Rule and Travel Rule, 31 C.F.R. 1010.410(e) and 1010.410(f), would still apply at certain thresholds, regardless of whether the redeemer is an account holder subject to CIP. Similarly, the transaction would still be subject to normal suspicious activity reporting, the PPSI's overall anti-money laundering compliance program, and OFAC screening and reporting.

Thus, the BSA will certainly address these one-off transactions, and in the appropriate way. But because GENIUS itself directs that the CIP programs are intended for "identification and verification of account holders with the permitted payment stablecoin issuer," *see* 12 U.S.C. 5903(a)(5)(v), there is no basis to extend those isolated transactions with a CIP protocol.

D. The Final Rule Should Allow and Facilitate the Use of Digital Identity Verification Methods and Privacy-Preserving Technologies

Request for Comment 5: *Should the regulatory text explicitly discuss digital identity solutions or verifiable credentials? How could it best do so given the range of tools on the market?*

Yes, the regulatory text should explicitly discuss digital identity solutions or verifiable credentials. As we have urged in previous related comment letters, FinCEN should confirm in this and other rule texts that responsible implementation and experimentation of new technology includes the freedom to use digital identity techniques without supervisory penalty.[7] Innovation by definition involves iteration. Supervisory expectations should accommodate the experimentation inherent in deploying new technology, including periods when a new tool is being calibrated or run in parallel with legacy systems. Indeed, another proposed rule from FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism Programs,"[8] identifies "machine learning, generative artificial intelligence (GenAI), digital identity, blockchain monitoring and analytics, or application programming interfaces (APIs)"[9] as relevant innovative approaches, and, most importantly, provides that institutions that "responsibly

[7] *See* Andreessen Horowitz, Comment Letter on FinCEN and OFAC Notice of Proposed Rulemaking: AML/CFT and Sanctions Compliance Program Requirements for Permitted Payment Stablecoin Issuers, FINCEN-2026-0100-0073, pp.14-17 (June 9, 2026); Andreessen Horowitz, Comment Letter on Innovative Methods To Detect Illicit Activity Involving Digital Assets, TREAS-DO-2025-0070-0209 (Oct. 17, 2025).

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

[9] *Id.* at 18712.

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."[10] We urge FinCEN and the Agencies to concretely confirm in the Final Rule that digital identity, in various forms discussed below, may be relied upon for meeting CIP requirements. We address more details responsive to RFCs 5, 6, and 8 below.

Request for Comment 6: *What are the benefits and risks of using digital identity solutions or verifiable credentials as part of verifying customers' identities?*

Request for Comment 8: *What, if anything, could be changed to make the proposed rule more conducive to industry innovation?*

1. Alternative Means of Digital Identity Verification

FinCEN and the Banking Agencies rightfully seek comment on the appropriateness of possible solutions for digital identity, or other verifiable credentials to be used in the CIP process. Proposed Rule § 1033.220(a)(2) would require the CIP to include risk-based procedures for verifying the identity of each customer to the extent "reasonable and practicable" sufficient to enable the PPSI to form a reasonable belief that it knows the customer's true identity.[11]

Traditionally, because of market practices and available technologies, financial institutions verified identity by visual examination of the customer's government-issued documents. Over time, those practices proved inefficient and unsuited to a growing electronic and virtual financial services industry. And, importantly, many of those approaches became susceptible to fraud, manipulation, and other activities that undermined their reliability.

The government has acknowledged that traditional approaches to identity verification have become increasingly difficult for several reasons.[12] Many institutions (including non-PPSI

---

[10] *Id*.

[11] Proposed Rule at 37270.

[12] *See, e.g.,* OCC, FDIC, NCUA, FinCEN (concurring), Exemption Order Related to TIN Collection and Customer Identification Program Requirements (June 27, 2025), available at https://www.fincen.gov/system/files/2025-08/CIP-TIN-Exemption-Order-final508.pdf (acknowledging that traditional approaches to customer identity verification have become increasingly challenging due to the growth of non-face-to-face account opening, rising identity theft risks, and evolving verification technologies); FinCEN, *Exceptive Relief for Casinos from Certain Customer Identity Verification Requirements*, FIN-2021-R001 (October 19, 2021), available at https://www.fincen.gov/system/files/administrative_ruling/2021-10-19/Casino%20Exceptive%20Relief%20101921.pdf (recognizing that non-documentary verification procedures can provide more comprehensive verification of an online customer's identity than the documentary methods currently required by FinCEN's regulations); FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004, (November 13, 2024), available at https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508F

financial institutions) have become remote-only. Remote verification (often by internet) has become commonplace for a whole range of institutions. For instance, many banks under the jurisdiction of the Agencies do not even have a physical presence, and do not require a physical presentation of documents to open an account. In fact, for many of these banks that have no brick-and-mortar presence, it would be impossible for them to physically review such documents. The same is true with online brokerage companies; certain residential loan originators; many money transmitters; and a host of other financial institutions covered by the BSA. And although in-person, document-verification techniques have largely remained static (with only a handful of exceptions), fraudsters and other actors, including "Fraud-as-a-Service" businesses,[13] have developed new technologies and entire businesses designed to produce false identification documents that are near perfect.

FinCEN has previously permitted financial institutions to verify customer credentials through electronic means. In providing interpretive guidance on CIP requirements under Section 326 of the USA PATRIOT Act, FinCEN stated that a bank may "obtain an electronic credential, such as a digital certificate, as one of the methods it uses to verify a customer's identity."[14] In that guidance, FinCEN reminded banks to ensure they have a reasonable belief that they know the true identity of the customer and advised banks to ensure that the third party uses the same level of authentication as the bank itself would use. Here, the Final Rule should include similar obligations on PPSIs to ensure that the PPSI has a reasonable belief that it knows the true identity of the customer and that the third party identification provider uses the same level of authentication as the PPSI itself would use. This aspect of the Final Rule would closely align with the risk-based and technology-neutral structure.

Further, this would align with the Final Rule's recognition of the growing presence of digital tools in the financial sector. FinCEN and the Agencies note that digital identity tools have become more sophisticated and more commonplace since the original bank CIP rule was adopted twenty years ago. The Agencies should seek to preserve the flexibility of means used to verify

---

INAL.pdf (recognizing that AI and deepfakes have complicated traditional identity-verification processes by enabling actors to circumvent existing authentication and customer identification controls).

[13] *See* Kennedy Meda, *Fraud-as-a-Service: Creating a new breed of fraudsters*, Thomson Reuters (Feb. 21, 2025), available at https://www.thomsonreuters.com/en/institute/articles/faas-new-fraudsters (describing fraud-as-a-service ("FaaS") as a "secretive industry in which cybercriminals offer tools, services, and support to fraudsters in exchange for payment" and that mid-market banks had experienced losses between $5 million and $10 million due to attacks by organized FaaS cybercriminal groups); *see also* Group-IB, *What is Fraud-as-a-Service? How the Dark Web Economy Industrialized Fraud* (Aug. 6, 2026), available at https://www.group-ib.com/resources/knowledge-hub/fraud-as-a-service/ (describing the intricate FaaS cybercrime model in which "skilled criminals build and sell fraud tools, while less skilled buyers use them{,}" leading to stolen data traded on "dark web markets, encrypted forums, and Telegram channels, then turned against banks, payment providers, e-commerce, and telecom"; further explaining that industries primarily targeted by FaaS are financial services, e-commerce, and telecommunications, noting that "financial services and internet services were the targets of more than 80% of all phishing in the Middle East and Africa in 2025").

[14] FinCEN, *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act* (Apr. 28, 2005) at Customer Verification FAQ 3.

customer identities, rather than prescribe a specific and exclusively permitted technology. A mobile ID issued by a state could constitute an "unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard" thereby satisfying the requirements under proposed § 1033.220(a)(2)(ii)(A).

Accordingly, the Final Rule should confirm that a state issued mobile identification card would satisfy the requirements of proposed § 1033.220(a)(2)(ii)(A), provided it is unexpired and bears a photograph or similar safeguard. This type of digital identity verification would not run counter to FinCEN's historical practices, but would rather be promulgated in harmony with previous interpretive guidance and regulations. This would also further FinCEN's stated pursuit of maintaining the flexibility relating to how a PPSI verifies a customer's identity. Finally, permitting verification through a mobile state identification would closely align with the Proposed Rule's risk-based and technology neutral structure.

2. Non-Documentary, Non-Governmental Means of Identity Verification

The Final Rule should approve alternative digital identity verification means beyond those just issued by state or national governments. In many instances, divulging the information contained within a government-issued ID, even when presented digitally, can compromise a customer's safety by exposing personally identifiable information and increasing the risk of financial harm, identity theft, fraud, and other unauthorized uses of that information.[15] For example, a government-issued mobile ID typically discloses a customer's full legal name, residential address, date of birth, photograph, and a unique government identification number in one disclosure. This bundle of sensitive personally identifiable information increases the customer's exposure to identity theft, stalking, or targeted fraud if that information is intercepted, mishandled, or retained longer than necessary by the PPSI. This collection and storage of sensitive data creates a serious risk of honeypots, which are likely to be exploited by malicious financial criminal actors.[16] To avoid these unwarranted vulnerabilities, the Agencies should consider alternative ways for a PPSI to digitally verify a customer's identity beyond simply government-issued identification records.

The Agencies wisely acknowledge that "[a] digital identity credential offered by a non-governmental entity that enables a person to prove that they are who they claim to be without revealing information other than that fact could, if appropriate as part of a risk-based procedure, be a non-documentary verification method." Proposed Rule at 37242. Digital identity credentials offered by a non-governmental entity that lets a person prove who they are without revealing extraneous information could, if appropriate under a risk-based procedure, serve as a

[15] *See* Treasury Dep't., *Treasury Directive 25-08* (Dec. 22, 2009, last edited July 16, 2024) available at https://home.treasury.gov/about/general-information/orders-and-directives/td25-08 (noting the significant financial losses and burdens to individuals affected by breaches of personally identifiable information).

[16] Narendran Vaideeswaran, *Honeypots in Cybersecurity Explained*, Crowdstrike (Jan. 16, 2025), available at https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/.

non-documentary verification method. There are several alternative, non-documentary means of verification that the Final Rule should consider.[17]

The Final Rule should permit PPSI digital identity verification based on identification credentials beyond a government-issued state mobile ID. Only a subset of states have implemented mobile driver's license programs, and rollout timelines vary widely.[18] Tying digital identity verification solely to state mobile ID would create an uneven system where customers from states that have not adopted mobile ID programs would face greater friction in verifying their identity. This issue can be resolved if the Final Rule permits non-documentary credentials for digitally verifying a customer's identity. These alternative means of verifying a customer's identity could include professional licensing credentials, third-party identity verification networks (*e.g.*, Login.gov, ID.me), mobile carrier-based verification, biometric credentials, healthcare or insurance credentials, and financial institution credentials. Before confirming an exhaustive list of alternative, non-documentary means of digitally verifying a customer's identity, FinCEN should engage in further rulemaking and comment periods to solicit industry feedback on alternative verification credentials. Further, expanding the scope of permitted digital verification methods aligns closely with the Proposed Rule's technology-neutral design. The identity verification permitted by the Final Rule should not be tied to any one credential type. By permitting a variety of different digital verification methods, the Final Rule would further its stated purpose of achieving a technology-neutral design.[19]

Additionally, the Final Rule should permit PPSIs to digitally verify a customer's identity through the use of decentralized identifiers ("DIDs") and verifiable digital credentials ("VDCs"). A DID is a unique ID that acts as "proof of ownership" over a digital identity of a subject, *i.e.*, a

---

[17] Treasury itself has recognized that digital identity verification need not rely exclusively on government-issued IDs. Indeed, in implementing ID.me identity proofing, Treasury provides alternative verification procedures. Concerns regarding the fraud and identity-theft risks associated with reliance exclusively on government issued ID have been increasingly recognized by regulators and policymakers. *See* Bill Fisher and Ryan Galluzzo, *Check Your Wallet? How Mobile Driver's Licenses are Changing Online Transactions*, National Institute of Standards and Technology (May 22, 2024) available at https://www.nist.gov/blogs/cybersecurity-insights/check-your-wallet-how-mobile-drivers-licenses-are-changing-online (noting that the efficacy of government issued driver's license verification procedures is being eroded by new technology like artificial intelligence).

[18] For the full list of the twenty participating states, please see Transportation Security Administration, Participating States and Eligible Digital IDs, available at https://www.tsa.gov/digital-id/participating-states.

[19] a16z notes that the Department of Treasury has consistently endorsed digital identity tools to enhance verification procedures across all financial institutions. *See* U.S. Department of the Treasury, *Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets* (Mar. 2026) at 22 (noting Treasury will "explore working with Congress on legislation to incentivize the development and integration of digital identity tools"); *see* FinCEN, *FinCEN Issues Analysis of Identity-Related Suspicious Activity* (Jan. 9, 2024) available at https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity ("Treasury and FinCEN recognizes that innovations in digital identity can strengthen anti-money laundering and countering the financing of terrorism compliance…"); Proposed Rule at 37241-42 ("FinCEN and the Agencies recognize the interest in leveraging verifiable credentials and digital identity as part of account opening procedures.").

person, organization, or thing.[20] DIDs point to "DID documents," which contain information explaining how to use the DID, such as a verification method.[21] Using the information recorded in the DID document, participants can verify a proof made by the DID subject, authenticating that the subject owns a particular digital identity.[22] A key feature of DIDs is that they are user-controlled authenticators—managed by their holder rather than a third party. VDCs are cryptographically-secured digital records that allow issuers to make verifiable attestations about an individual, while making it possible for verifiers to authenticate this information without relying on intermediaries.[23] For example, a PPSI could attest to a person's account history or a university could attest to a degree. VDCs are stored in a user's wallet, and can be associated with a DID. A person can then present proofs regarding their credentials to satisfy a verifier's requirements.[24] Ultimately, the Final Rule should permit a variety of alternative non-documentary means of digitally verifying a customer's identity, extending the scope of permissible verification methods far beyond merely that of a state-issued mobile ID. By permitting PPSIs to verify identities through DIDs, VDCs, other non-government credentials, or reliance on qualified PPSI verification, the Final Rule would close inefficiency gaps in customer verification, while still effectively safeguarding the industry against financial criminal actors.

3. Zero-Knowledge Proofs and Privacy-Preserving Digital Identity Verification

The Proposed Rule in § 1033.220(a)(3) states that the CIP must include procedures for making and maintaining a record of all information obtained by the PPSI through the CIP. This Proposed Rule would, at a minimum, require certain basic identifying information used by the PPSI in verifying the identity of the customer. The Final Rule should expressly permit PPSIs to obtain this basic identifying information through zero-knowledge proofs or other means of digital identity attestation, especially those with privacy-preserving technologies.[25] A

[20] World Wide Web Consortium (W3C), *Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations*, W3C Recommendation (July 19, 2022), available at https://www.w3.org/TR/did-1.0/.

[21] *Id*.

[22] *Id.*

[23] *Id.*

[24] Importantly, methods exist to help preserve the privacy of individuals using this identity architecture. For example, individuals can generate a new DID for each relationship or interaction, helping to prevent reidentification via correlation across multiple DIDs.

[25] The Department of Treasury has previously endorsed the use of zero-knowledge proofs as a means of reliably identifying a customer, without unnecessarily requiring the excessive disclosure of personally identifiable information. *See* U.S. Department of the Treasury, *Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets* at 18 (Mar. 6, 2026) (discussing zero-knowledge proofs as enabling customers to "prove that they are who they claim to be without revealing information other than that fact"). Additionally, FinCEN has already recognized the potential utility of privacy-enhancing technologies, including zero-knowledge proofs, in the context of digital identity verification. *See* FinCEN, *FDIC FinCEN Digital Identity Tech Sprint – Key Takeaways and Solution Summaries* (Sep. 9, 2022), available at https://www.fincen.gov/news/news-releases/fdic-fincen-digital-identity-tech-sprint-key-takeaways-and-solution-summaries.

zero-knowledge proof is a cryptographic technique which allows a PPSI to reasonably determine the identity of a customer without revealing private information. While the concept of zero-knowledge proofs has been around for decades, widespread implementation and use of zero-knowledge proofs have gained traction in parallel with advancements in cryptography. The four key types of zero-knowledge proofs include interactive zero-knowledge proofs, non-interactive zero-knowledge proofs, zk-SNARKs, and zk-STARKs.

- **Interactive Zero-Knowledge Proofs**: An interactive zero-knowledge proof involves several rounds of communication between a prover and verifier. The prover convinces the verifier of the validity of the prover's identity without revealing any additional information.[26]
- **Non-Interactive Zero-Knowledge Proofs**: In contrast, a non-interactive zero-knowledge proof wholly eliminates the need for multiple rounds of communication between the prover and the verifier. Instead, the verifier relies on a single proof generated by the prover to confirm the identity of the prover.
- **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge)**: At a high level, zk-SNARK refers to a proof mechanism where one can prove possession of information like a secret key or password without actually revealing that information and without any interaction between the prover and verifier.[27] These represent a complex computation that is transformed into mathematical constraints. The "prover" generates a compact (succinct) proof that these constraints were satisfied, and the verifier checks the proof much faster than re-running the computation. The zk-SNARK is considered "succinct" because the zero-knowledge proof can be verified within a few milliseconds. And the zk-SNARK is "non-interactive" because it does not require any communication between the prover and the verifier.
- **zk-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge):** Similar to zk-SNARKs, zk-STARKs are cryptographic tools that allow for the generation of proofs of knowledge without divulging sensitive information.[28] zk-STARKs are designed to be highly scalable, making them especially useful for large-scale decentralized systems and applications. Unlike other zero-knowledge proof systems, zk-STARKs are transparent, meaning the entire proof generation process is publicly verifiable. This ensures that the proof's integrity can be independently verified without relying on a trusted third party.

Zero-knowledge proofs like zk-SNARKs and zk-STARKs, as well as other privacy-preserving identity systems, could achieve compliance while reducing unnecessary data exposure. Encouraging the use of privacy-enhancing technologies for digital identity verification

[26] 1Kosmos, *What is a Zero-Knowledge Proof? How It Works*, available at https://www.1kosmos.com/resources/security-glossary/zero-knowledge-proof.

[27] Mina Foundation, *What are zk-SNARKs?* (June 10, 2021), available at https://minaprotocol.com/blog/what-are-zk-snarks.

[28] Julieta Cura, *What means zk-STARK?* Extrimian (Apr. 29, 2024), available at https://extrimian.io/wikis/zk-starks/.

advances several policy goals simultaneously. First, it promotes a risk-based approach to the processing of personal data by minimizing the amount of sensitive data stored by PPSIs. Treasury and FinCEN have consistently endorsed risk-based customer identification and verification frameworks that focus on achieving a reasonable belief regarding a customer's identity. For example, existing CIP regulations promulgated by FinCEN are already risk-based, as the current CIP rule for banks requires "risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable."[29] Further, in its 2026 AML/CFT modernization proposal, FinCEN stated that financial institutions should incorporate risk-based AML compliance frameworks, underscoring the importance of balancing the protection and privacy needs of customers' personal data.[30] Privacy-preserving technologies could advance those objectives by enabling verification of required identity attributes while limiting disclosure of unnecessary personal data. Put simply, zero-knowledge proofs align with the principle of collecting only information necessary for a regulatory purpose, and only enough information such that the PPSI can form a reasonable belief that it knows the true identities of its customers.

Second, a Final Rule permitting the use of zero-knowledge proofs and privacy-preserving technologies would promote enhanced cybersecurity practices of PPSIs. If the Final Rule required PPSIs to document and store vast amounts of personally identifiable information stored digitally on private servers, PPSIs would become prime targets for cybercriminals. Limiting collection and retention of identity documents reduces widespread breaches of personal data. The Department of Treasury has consistently emphasized the importance of a financial institution's cybersecurity infrastructure. In its 2025 Financial Services Sector Risk Management Plan, the Department of Treasury recognized that financial institutions operate in a highly interconnected environment where vulnerabilities at one institution can create systemic risks across the sector.[31] For this reason, the Treasury emphasized the importance of financial institutions maintaining comprehensive and effective cybersecurity frameworks. Accordingly, a Final Rule that permits the use of zero-knowledge proofs and privacy-preserving technologies would harmoniously accord with Treasury's practice of encouraging financial institutions to maintain robust and effective cybersecurity safeguards.

Finally, a Final Rule permitting the use of privacy-preserving technologies to verify a customer's identity would avoid requiring customers to provide and PPSIs to store an overly burdensome amount of sensitive personal information. To the extent these technologies enable a PPSI to form a reasonable belief that it knows the customer's true identity, their use would be consistent with the proposed rule's flexible, risk-based approach to customer identification. Zero-knowledge proofs and other privacy-preserving technologies that provide the PPSIs with a reasonable belief that it knows the true identity of the customer would promote the proposed

[29] 31 C.F.R. 1020.220.

[30] *Fact Sheet: Proposed Rule to Fundamentally Reform Financial Institution AML/CFT Program*, U.S. Department of the Treasury's Financial Crimes Enforcement Network (April 2026).

[31] U.S. Department of the Treasury, *Financial Services Sector Risk Management Plan* (Jan. 2025).

rule's goal of enhancing effective customer identification through flexible, risk-based verification processes.

Indeed, privacy-preserving technology should not be treated as inherently suspicious – FinCEN should consider including a statement in the final rule or elsewhere that the use of privacy-preserving technologies, such as a shielded protocol, zero-knowledge proof, self-custody wallet, selective-disclosure credential, or similar technology does not, standing alone, establish heightened customer risk justifying enhanced due diligence and record collection.

We understand, of course, that CIP programs are intended for verification of an extensive set of facts for customer onboarding: name; date of birth/corporate formation; address; principal place of business (for businesses); identification number; and other information. As such, there may be some uses of the technology that might be suitable for some purposes (such as the determination of whether the person is over eighteen years old without disclosing her date of birth, or whether the person is a resident of New York without disclosing his actual address), but might not be suitable for other purposes (such as CIP). That said, FinCEN and the Banking Agencies might issue Requests for Information to the industry for innovative solutions and technologies for CIP compliance.

4. The Final Rule Should Avoid Documentary Capture Requirements that Could Lead to Identity Fraud

The Treasury Department has recognized the increased exposures to identity theft risk and fraud that individuals face given the rise in the use of deepfake media created with generative artificial intelligence tools. In a November 2024 alert, Treasury warned financial institutions that "bad actors are seeking to exploit (GenAI) to defraud American businesses and consumers, to include financial institutions and their customers."[32] FinCEN observed an increase in suspicious activity reporting by financial institutions describing the suspected use of deepfake media, "particularly the use of fraudulent identity documents to circumvent verification and authentication methods."[33]

Further, the Financial Action Task Force ("FATF") recognized in its 2025 report "Horizon Scan: Artificial Intelligence and Deepfakes" the growing risk created by financial criminals' use of deepfakes to sidestep an institution's customer due diligence infrastructure and "impersonate individuals, manipulate biometric authentication, or support social engineering

[32] FinCEN, *FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions* (Nov. 13, 2024), available at https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial.

[33] *Id*.

schemes."[34] Recognizing the increased opportunities that criminals have to undermine authentication and verification procedures, the FATF stated that it is now "more vital than ever for institutions to implement a sound CDD framework that considers this new threat landscape through this informed risk-based approach."[35] The FATF's *Horizon Scan* report emphasizes the need for enhanced vigilance within an institution's due diligence framework.

Accordingly, the Final Rule should reflect this recognized and growing risk by preserving flexibility within a PPSI's CIP rather than requiring additional documentary capture. Deepfakes and other AI-generated fraud schemes can undermine both documentary and non-documentary verification methods, making the collection of additional documents an unreliable standalone solution. Imposing unnecessary and additional documentary collection requirements in a PPSI's identification program will only provide further opportunities for criminal actors to exploit document-based verification processes by using AI-generated deepfakes. The Final Rule should therefore account for this by preserving a PPSI's flexibility in verification procedures and minimizing requirements for unnecessary documentary capture. This approach will better advance the Final Rule's objective of effective customer identification while minimizing unnecessary document collection burdens. Thus, the Final Rule should avoid imposing unnecessary documentary verification mandates that would otherwise create vulnerabilities to false verification threats from a malicious actor's use of AI-generated fraud.

E. Reliance upon state-qualified PPSIs

***Request for Comment 7**: What is the expected likelihood that a PPSI would rely on another PPSI's CIP or the CIP of another Federal functionally regulated financial institution's CIP?*

Proposed Section 1033.220(a)(6) permits a PPSI to rely upon another institution's CIP program, but only if the relied-upon institution is regulated by a Federal functional regulator (as defined in 31 C.F.R. 1010.100(r)). This results in an asymmetry: a state-qualified PPSI may rely on a bank-subsidiary PPSI or federally-regulated PPSI, but not the reverse, even though both are subject to the same CIP regulation. Indeed, the Proposed Rule also expressly permits use of third-party service providers.[36] But although the state-qualified PPSI may use exactly the same service provider in exactly the same way, the bank-subsidiary PPSI could not rely on the CIP determinations of the state-regulated PPSI.

The Proposed Rule correctly acknowledges this as a "disparity." 91 Fed. Reg. at 37243. To correct this disparity, the Final Rule should permit federal bank-subsidiary PPSIs to rely upon the CIP programs of any other "qualified" PPSIs, including those covered by state regulators,

[34] Financial Action Task Force, *Horizon Scan: Artificial Intelligence and Deepfakes* (2025) at 3, available at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Horizon%20Scan%20AI%20and%20Deepfakes.pdf.coredownload.inline.pdf.

[35] *Id.* at 6.

[36] Proposed Rule at 37243 and n.82.

that require their customers meet a defined standard of verification. FinCEN should engage in further rulemaking and comment periods to invite industry feedback on what the "defined standard of verification" should be and what could theoretically constitute a "qualified" PPSI. As a starting point, the defined standard of verification could be based on the National Institute of Standards and Technology ("NIST") assurance levels, and a qualified PPSI could be one that is registered with and has been vetted by FinCEN.[37] And any reliance must be reasonable under the circumstances, *see* Proposed Rule at 31 C.F.R. 1033.220(a)(6)(i); the PPSI must be subject to a CIP rule; and the parties enter into a contract certifying the implementation of an AML/CFT program, and that the relied-upon party agrees to perform the other party's CIP requirements, *see* Proposed Rule at 31 C.F.R. 1033.220(a)(6)(iii).

This approach would be consistent with how the government has previously addressed entities without a Federal Functional regulator. For instance, in its *Customer Identification Program, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator*,[38] FinCEN amended 31 C.F.R. 1020.220 so that it covers state-regulated banks under CIP rules to be identical to those with Federal charters.[39]

F. Express codification of the Enterprise-wide CIP Allowance

Similarly, the Final Rule should provide explicit authorizations for enterprise-wide CIP programs. For instance, if a federally-chartered bank has a subsidiary PPSI, the bank's CIP program (and AML program more broadly) should be allowed to cover both the "banking" and stablecoin parts of the business under a unified, company-wide system. Such an approach allows enhanced efficiency (for instance, by allowing shared personnel and transaction monitoring technology) while also promoting effectiveness (by detecting potential discrepancies or sharing unusual or suspicious activities across systems, for example). Indeed, many financial institutions share their AML programs across business lines and throughout enterprise-wide systems for exactly these reasons.

Noting that "FinCEN and the Agencies recognize the value of enterprise-wide compliance efforts," the Preamble to the Proposed Rule permits depository institutions with CIP

---

[37] *See* Bill Hughes, *Stop verifying the same person five times*, Consensys (May 13, 2026) available at https://consensys.io/blog/portable-kyc-fincen-identity-verification. Relatedly, a FinCEN observed pilot program is testing "whether completed verification work can be documented in standardized records and evaluated by other financial institutions." *See also* PYMNTS, *Banks Target Repeat Checks That Drive Customers Away* (Aug. 19, 2026), available at https://www.pymnts.com/authentication/digital-identity/2026/banks-target-repeat-checks-that-drive-customers-away

[38] *Financial Crimes Enforcement Network; Customer Identification Program, Anti-Money Laundering Programs, and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator*, 85 Fed. Reg. 57129 (Dep't Treas. Sep. 15, 2020).

[39] As a corollary, PPSIs should be allowed to rely on private banks and trust companies' CIP programs, even though such entities do not have a federal functional regulator but are still subject to CIP requirements.

programs to extend their AML programs (including CIP programs) to their PPSI subsidiaries.[40] It also allows national trust banks to maintain a single, enterprise-wide CIP.

Although noted in the preamble, this allowance is not codified in the Proposed Rule itself.[41] *See* Proposed 31 C.F.R. 1033.220(a)(1). Therefore, we respectfully submit that the Final Rule includes this clarifying language so that institutions will be able to share such programs.

IV. Conclusion

A16z is deeply committed to the development of a legal and regulatory framework for stablecoins and other digital assets, which we believe is critical to fostering innovation while protecting market participants and the safety of the financial system. And within that framework, a sensible, practical, and effective set of CIP requirements for PPSIs is essential. To that end, we hope that our observations and comments will be of assistance to the Agencies.

We greatly appreciate the opportunity to provide comments on these important matters, and we look forward to continued engagement with the government 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

[40] Proposed Rule at 37241 ("Where a PPSI is a subsidiary of an insured depository institution, FinCEN and the Agencies anticipate that the enterprise may elect to extend a single AML/CFT program to both entities and that doing so would be permissible so long as a comprehensive AML/CFT program is reasonably designed to identify and mitigate the risks posed by the different aspects of each entity's business and activities and satisfies each of the risk-based AML/CFT program and other applicable BSA and GENIUS Act requirements…".).

[41] *Id.*