NOTABENE INC, LANA SCHWARTZMAN, ET. AL.

Proposal and Comment Information

Title: Permitted Payment Stablecoin Issuer Customer Identification Program, R-1885

Comment ID: FR-2026-0005-01-C17

Submitter Information

Organization Name: Notabene Inc

Organization Type: Company

Name: Lana Schwartzman, et. al.

Submitted Date: 08/21/2026

Notabene Inc. is respectfully submitting these comments in response to the joint notice of proposed rulemaking (the "NPRM") issued by the Financial Crimes Enforcement Network in coordination with the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. The NPRM proposes customer identification program requirements for permitted payment stablecoin issuers under the Guiding and Establishing National Innovation for U.S. Stablecoins Act. As the NPRM is being issued jointly by these five agencies, Notabene is submitting this letter to each agency's respective comment docket.

Response to the Joint Notice of Proposed Rulemaking: Permitted Payment Stablecoin Issuer Customer Identification Program

Submitted by: Notabene, Inc. via Regulations.gov
Date: August 21, 2026
Contact: Lana Schwartzman, VP Global Regulatory & Compliance Strategy, lana@notabene.id

The Honorable Andrea Gacki, Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
Post Office Box 39
Vienna, VA 22183

The Honorable Jonathan V. Gould
Comptroller of the Currency
Office of the Comptroller of the Currency
400 7th Street SW, Suite 1E-F216
Washington, DC 20219

The Honorable Kevin Warsh, Chairman
Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

The Honorable Travis Hill, Chairman
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

The Honorable Kyle S. Hauptman, Chairman
National Credit Union Administration
1775 Duke Street
Alexandria, VA 2231

Re: Permitted Payment Stablecoin Issuer Customer Identification Program (FinCEN Docket FINCEN-2026-0101, RIN 1506-AB74; OCC Docket OCC-2026-0331, RIN 1557-AF53; Board Docket R-1885, RIN 7100-AH18; FDIC RIN 3064-AG28; NCUA Docket NCUA-2026-0793, RIN 3133-AG09)

Executive Summary

Dear Director Gacki, Comptroller Gould, and Chairmen Warsh, Hill, and Hauptman:

Notabene, Inc. submits this letter in response to the joint proposed rule issued by the Financial Crimes Enforcement Network, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the National Credit Union Administration implementing the customer identification program requirement for permitted payment stablecoin issuers under the Guiding and Establishing National Innovation for U.S. Stablecoins Act, 91 Fed. Reg. 37,234 (2026).

We support the proposal and the judgment at its center. The agencies have concluded that a customer identification program obligation attaches where an issuer has a direct relationship with a person, and does not attach where a person only contact with the issuer runs through a

smart contract. That is the right line. Extending customer identification to secondary market activity would make every issuer the identity authority for its entire token float, duplicate work already performed by the institutions holding the customer relationship, and generate identity records with no transactional context attached to them.

Drawing that line correctly does create an obligation to be clear about where secondary market risk is addressed instead. It is addressed at the intermediary layer, at the moment of transfer, through the requirements already sitting in 31 CFR chapter X. Our comments below develop that point and address the questions where our position as compliance infrastructure between more than 2,100 institutions gives us something specific to contribute.

What we recommend:

1. Do not extend customer identification program requirements to secondary market activity. Address secondary market risk through transaction-level controls at the intermediary layer under chapter X, where the customer relationship and the transaction data already sit (Question 1).
2. Retain the smart contract carve-out in the account definition and the secondary market exclusion in the customer definition as drafted (Questions 1 and 2).
3. Clarify that transmitting identity information, compliance data or authorization messages relating to a transfer is not transferring digital assets to a third party under the digital asset service provider definition (Question 2).
4. Retain formal relationship as the foundation of the account definition, and publish hallmarks in guidance rather than regulatory text, including registration or allowlisting of settlement addresses with the issuer (Question 3).
5. State in the regulatory text that a person redeeming directly with an issuer without a prior relationship opens an account, and address verification timing for one-off redemptions (Question 4).
6. Keep the verification provisions technology-neutral, and add one affirmative sentence confirming that a digital identity credential may satisfy documentary or non-documentary verification where the issuer establishes its assurance level. Handle standards in guidance (Questions 5 and 6).
7. Recognize privacy-preserving verification techniques built on open standards, including cryptographic name matching, as a valid means of confirming identity correspondence between institutions, provided the underlying information continues to be collected, retained and available to competent authorities (Questions 6 and 7).
8. Confirm that an issuer is not required to re-verify the customers of a counterparty institution that has performed equivalent identification. The intended mechanism is identification by the institution holding the customer relationship, transmission of the required information, and appropriate due diligence on the counterparty institution (Questions 1 and 7).

9. Extend reliance under section 1033.220(a)(6) to state qualified payment stablecoin issuers supervised under a certified state regime, and open a route for foreign financial institutions subject to AML/CFT requirements consistent with FATF standards (Question 7).
10. Confirm in the regulatory text that engaging a third-party provider to perform or support a customer identification procedure is outsourcing rather than reliance, and does not trigger the contract and annual certification conditions (Question 7).
11. Recognize pre-transaction, authorize-then-settle controls as affirmative evidence of program effectiveness, and account for blockchain addresses registered for mint and redeem within the identifying information a customer identification program addresses, paired with verifiable identification of the institution servicing the address (Question 8).
12. Align the five-year customer identification retention period with chapter X transaction recordkeeping, and coordinate the effective date to run from the latest of the related GENIUS Act rulemakings (Question 8 and general comment).

Introduction and Overview

Notabene, Inc. is a global compliance infrastructure provider for digital asset transfers. Our platform enables virtual asset service providers, financial institutions and payment stablecoin issuers to identify counterparties, exchange required originator and beneficiary information, screen for sanctions exposure, and authorize transactions before settlement, in line with FATF Recommendation 16 and equivalent national frameworks, including the requirements at 31 CFR chapter X (31 CFR 1022.400,1010.410(e)-(f). More than 2,100 institutions rely on our network, representing over 2.2 trillion dollars in annualized transaction volume across more than 100 jurisdictions.

Notabene also introduced and maintains the Transaction Authorization Protocol, an open, blockchain-agnostic standard providing a private messaging layer through which the parties to a transaction identify one another and authorize or reject a transfer before final settlement. The protocol is designed to carry the information required under Recommendation 16 across multi-step chains combining virtual asset and fiat legs, and to interoperate with established messaging standards including ISO 20022.

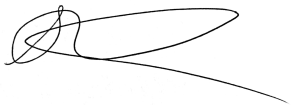
We commented in detail on the Treasury AML and sanctions compliance proposed rule published by FinCEN and OFAC on April 10, 2026 (91 FR 18582), and on the parallel OCC and FDIC proposals for permitted payment stablecoin issuers. We also responded to the FATF public consultation on draft Guidance for the implementation of Recommendation 16 in August 2026. Our positions here are consistent with those submissions, and we identify the points of overlap where they bear on the questions the agencies have asked.

Our comments fall into three groups. The first concerns the boundary of the customer identification obligation and what sits on the other side of it (Questions 1 through 4). The second concerns identity verification methods and how the rule should treat digital identity

credentials without freezing a technology into the Code of Federal Regulations (Questions 5 and 6). The third concerns reliance, which we regard as the provision with the widest gap between its potential and its likely uptake as drafted (Questions 7 and 8).

We appreciate the opportunity to comment and would welcome further discussion with agency staff, in particular on examination expectations for transaction-level identity and authorization controls in payment stablecoin systems.

Thank you,



Lana Schwartzman
VP, Global Regulatory and Compliance Strategy
Notabene, Inc.

Catarina dos Santos Veloso

Catarina Veloso
Director, Regulatory and Compliance
Notabene, Inc.

General Comment: Where Identity Attaches in a Payment Stablecoin Transfer

An issuer sees its primary market clearly and its secondary market barely at all. That is a structural feature of the design, not a deficiency in any particular issuer program. Once a token is in circulation, the parties with the customer relationship, the identity records and the transaction context are the exchanges, custodians, payment firms and other institutions holding the wallets on each side. Those institutions already carry obligations under chapter X to identify their customers, screen counterparties and transmit originator and beneficiary information with qualifying transfers.

This is why the customer identification program should stay where the agencies have put it. Identity attaches at two points in a payment stablecoin system. It attaches when a person opens a direct relationship with the issuer, which this rule governs. It attaches again when a person transacts through an institution, which chapter X governs. Between those two points is the smart contract, which is where identity does not attach and cannot be made to.

We would encourage the agencies to state this layering plainly in the final rule preamble. Issuers and their supervisors will read a rule that declines to reach secondary market activity, and some will read it as a statement that secondary market activity carries no identity obligation at all. It carries a substantial one. It simply falls on a different party.

General Comment: Identification Belongs to the Institution Holding the Relationship

A related point runs through several of our answers and is worth stating once at the outset, because it explains why we treat the reliance provision as the most consequential drafting decision in the rule.

A customer identification framework works on the premise that the institution holding the customer relationship performs the identification, transmits the required information onward, and applies appropriate due diligence to the institutions it deals with. It does not contemplate each institution in a chain re-verifying the customers of the institution before it.

When re-verification becomes the working assumption, two things happen, and we observe both across our network. Institutions perform duplicative due diligence on the end customers of their counterparties, frequently because a banking partner requires direct identification of each underlying end customer rather than accepting verified transfer information together with due diligence on the counterparty institution. That duplication is costly and does not improve the quality of the information available. Separately, where an institution cannot establish an information-carrying connection across a leg of a transaction, it substitutes a bilateral commercial arrangement and treats the counterparty institution simply as its own customer. That simplifies the immediate relationship and obscures the actual chain, because the underlying originator or beneficiary becomes invisible to institutions further along it.

Neither outcome improves identification. Both reduce transparency, and both push institutions away from open, interoperable networks toward closed structures. We raised the same concern with the FATF in our response to its draft Guidance on Recommendation 16, recommending that the Guidance expressly reaffirm that an institution is not required to re-verify the end customers of its counterparties. We recommend the agencies confirm the equivalent principle here. An affirmative statement gives issuers an authoritative basis for responding to external requirements, including requirements imposed by banking partners, that would otherwise push them toward duplicative verification or closed-loop structures.

General Comment: Effective Date and Sequencing

We support the proposed twelve month compliance period. We recommend the period run from the latest of the final rules in the linked GENIUS Act package rather than from this rule alone.

This rule borrows its foundational definitions from the PPSI AML/CFT proposal, sits inside a part 1033 created by that proposal, and operates alongside the FinCEN and OFAC rule of April 10, 2026 and the parallel prudential frameworks at the OCC, FDIC, Board and NCUA. An issuer cannot finalize a customer identification program design until it knows what counts as a payment stablecoin issuer, what its program obligations are, and which supervisory framework applies. A staggered sequence would have issuers build against a moving target and rebuild as each rule lands, at real cost and no compliance benefit.

Stated precisely, we recommend the compliance date run twelve months from the latest of the effective date of the final FinCEN and OFAC rules implementing the GENIUS Act, the effective date of the OCC final rule adopting the part 15 framework, and the effective dates of the final AML/CFT and sanctions compliance rules of the FDIC, the Board and the remaining prudential regulators. The GENIUS Act directs the agencies to issue these rules in coordination, and a coordinated compliance date follows from that direction.

Question 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. We would note first that the question may be narrower than it appears. The GENIUS Act directs a permitted payment stablecoin issuer to maintain a program verifying the identities of account holders with the issuer, 12 U.S.C. 5903(a)(5)(A)(v). That language ties the obligation to the account relationship. It does not extend to the population of persons holding a token already issued into circulation, and we do not read it as authorizing an obligation of that scope. The policy analysis below leads to the same conclusion, but the statutory limitation reaches it first.

We agree with the agencies assessment and would put it slightly more sharply. A customer identification program is an account-opening control. Its entire mechanism depends on a

moment where the institution has something the person wants and can condition it on the production of verified identity information. In secondary market activity that moment does not exist. The issuer is not a party, has nothing to withhold, and receives nothing from the transfer beyond what the public ledger already shows. An obligation without a point of leverage produces paperwork rather than identification.

The drawbacks of extending the requirement are substantial. An issuer would become the identity authority for every holder of its token, a population the agencies estimate in the hundreds of millions against a primary market measured in the hundreds of thousands. It would duplicate identity work already performed by the exchange or custodian holding the relationship, without improving on it, since the issuer would be verifying at a distance and after the fact. Issuers would face a compliance obligation with no operational route to satisfy it, which is a poor foundation for a supervisory regime. And activity would move toward issuers outside U.S. supervision, which reduces visibility rather than increasing it.

The important point is what follows from declining to extend the obligation. The typologies the agencies list in the preamble, including fraud and scam proceeds, DPRK-linked laundering networks, narcotics proceeds and sanctions evasion, overwhelmingly move through the secondary market. While customer identification programs do not cover secondary market activity, other regulatory mechanisms do.

Transaction-level controls reach there, and they work. In a transfer between two hosted wallets, an institution sits on at least one side and usually both, each with a verified customer and each subject to chapter X. At the moment of transfer those institutions can identify the counterparty institution, exchange required originator and beneficiary information, screen both parties against sanctions lists, and verify that the beneficiary details match before the transaction reaches the chain. This is not theoretical. Within our network, participating institutions have blocked over $757 million in transfers where beneficiary details failed verification, indicating potential fraud or misdirection, and the share of institutions blocking withdrawals on failed verification continues to grow.

Timing is what makes this the right control for the asset class. Blockchain settlement is irreversible. A control applied after settlement documents a loss. A control applied before settlement prevents one. Customer identification at the issuer, however well executed, sits upstream of the transaction and cannot substitute for a check made at the point of transfer.

One category of issuer-level control does exist in the secondary market and should be kept distinct. Most issuers retain the technical ability to freeze balances or blocklist addresses through the smart contract, and the GENIUS Act requires the technological capability to comply with lawful orders, a requirement proposed section 1033.220(c) preserves. That is a sanctions and law enforcement control. It should not be recharacterized as a customer identification requirement, and the customer identification rule should not become the vehicle for expanding it.

We therefore recommend the agencies retain the boundary as proposed, and use the final rule preamble to identify chapter X transaction-level obligations as the mechanism addressing secondary market risk.

Question 2

> *Should FinCEN and the Agencies refine or clarify its definitions of account, customer, or digital asset service provider? Are additional definitions needed?*

The definitions of account and customer are well constructed and we do not propose substantive change to either. The carve-out for activity involving the issuer only through a smart contract, and the exclusion from customer of a person acquiring or redeeming other than directly from or to the issuer, together do the necessary work. Retaining both is more important than any refinement we could suggest.

We recommend two clarifications to the digital asset service provider definition.

The first concerns limb C, transferring digital assets to a third party. Read against the rest of the definition the intended meaning is clear, and it concerns movement of the asset. Read on its own by a compliance or examination team, the phrase is capable of a wider reading that reaches parties who transmit information about a transfer rather than the transfer itself.

The distinction we are drawing is one FinCEN has drawn before. The money transmitter definition at 31 CFR 1010.100(ff)(5)(ii)(A) excludes persons providing delivery, communication or network access services used to support money transmission, and FinCEN guidance FIN-2019-G001 confirms that suppliers of communications, hardware or software tools are engaged in trade rather than money transmission where they do not accept and transmit value themselves. The reasoning applies directly here. Treating the transmission of information about a transfer as the transfer of a digital asset would collapse a distinction that already runs through chapter X.

The distinction has practical consequence in this rule, because proposed section 1033.100(a)(1)(v) makes the provision of authorized digital asset service provider services an activity capable of forming an account. An issuer engaging a compliance messaging provider should not be left uncertain whether it has opened an account with that provider, and a compliance messaging provider should not be left uncertain whether it has become a digital asset service provider. We recommend a sentence in the regulatory text or, at minimum, in the preamble, confirming that transmitting identity information, compliance data or authorization messages relating to a transfer of digital assets does not constitute transferring digital assets to a third party.

The point is not confined to this rulemaking. In our response to the FATF draft Guidance on Recommendation 16 we recommended that the messaging, routing and transaction-authorization infrastructure developed to operationalize Recommendation 16 for virtual assets be recognized within the payment market infrastructure framework, on the basis that these providers are not the obliged entities responsible for compliance but supply the

infrastructure through which obliged entities discharge their obligations at scale. The same category distinction is what we ask the agencies to preserve here. A framework that recognizes compliance infrastructure as its own category, distinct from the institutions it serves, encourages convergence on interoperable standards. A framework that leaves the category ambiguous encourages fragmented, closed networks instead.

The second clarification concerns overlap with existing status. An issuer authorized by its regulator to conduct digital asset service provider activity may also meet the definition of money transmitter under 31 CFR 1010.100(ff)(5) for the same activity. The proposal does not say which framework governs. Consistent with the position we took in our comments on the OCC part 15 proposal, we recommend the agencies confirm that a permitted payment stablecoin issuer looks to the part 1033 framework for its Bank Secrecy Act obligations, so that a single entity is not assessed twice against two rulebooks for one activity.

On additional definitions, we do not think a new definition is required, but we do recommend the reliance and outsourcing distinction described in the preamble to section 1033.220(a)(6) be carried into the regulatory text. See our response to Question 7.

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

Retain it. The strongest argument for retention is one the agencies make themselves and which deserves more weight than it usually receives. Reliance under section 1033.220(a)(6) works only where the relied-upon institution account concept lines up with the relying institution. Every other customer identification rule under the Bank Secrecy Act is built on formal relationship. Introducing a different foundation here would create an interpretive seam at exactly the point where two institutions have to agree on what was covered.

Neither alternative improves matters. Contractual relationship is under-inclusive, since relationships are frequently established through an onboarding and approval process rather than a negotiated bilateral agreement, and it is simultaneously over-inclusive in an unhelpful direction, since accepting terms of service on a public webpage forms a contract without forming anything resembling an account. Business relationship is vaguer than formal relationship rather than clearer.

On hallmarks, we offer the following from what we observe operationally. A formal relationship is generally present where one or more of these are true:

- The person has completed an onboarding or approval process with the issuer and accepted the issuer terms for direct dealing.

- The person is able to instruct the issuer to mint, redeem, convert, repurchase or burn.
- The person has registered or allowlisted one or more blockchain addresses with the issuer for settlement of mint or redeem instructions.
- The person has designated a fiat funding or payout account with the issuer.
- The person holds credentials or API access to an issuer-operated interface.
- The issuer holds stablecoins, reserve assets or private keys for the person.
- There is a fee, commission or other commercial arrangement between them.

We would put particular weight on the allowlisted settlement address. It is verifiable, durable, recorded by the issuer as a matter of ordinary operations, and it is the one hallmark that ties a verified identity to on-chain activity. It also distinguishes cleanly between the primary market and the secondary market, since a person transacting only in the secondary market has no reason to register an address with the issuer and no route to do so.

Examples belong in guidance rather than regulatory text. Issuer business models are still forming, the agencies expect roughly fifty issuers in the first three years, and a list in the Code of Federal Regulations would be harder to update than the market it describes.

Question 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?*

Yes, and we recommend the clarification sit in the regulatory text rather than the preamble alone.

Redemption is the point at which a payment stablecoin converts back into reserve assets and value leaves the token system. Of every interaction available in the primary market it carries the most direct illicit finance exposure, because it is the off-ramp. If the rule places an identity checkpoint anywhere, this is the place with the strongest claim to it.

The proposal reaches the right answer already. A first-time redeemer establishes a formal relationship, opens an account and becomes a customer. But that answer currently sits in preamble discussion framed as a question. With roughly fifty issuers building programs against this rule, and no supervisory history to draw on, an unstated answer becomes fifty answers. We recommend the account definition or the customer definition state directly that a person who instructs the issuer to redeem, and who does not already hold an account, opens one by doing so.

We also recommend the rule address verification timing for this case. Proposed section 1033.220(a)(2)(ii) allows verification within a reasonable period after the account is opened, which is a sensible standard for a continuing relationship where the institution retains leverage and contact. A one-off redemption ends before any reasonable period elapses. Proceeds are released and the relationship is over. We recommend the rule require that a customer

identification program address, on a risk basis, verification before or contemporaneous with the release of redemption proceeds where the account is opened for redemption alone.

Two points make this more workable:.

- First, most first-time redeemers do not arrive unknown. They arrive from an exchange, custodian or other institution that has already performed customer identification to a standard equivalent to this rule. Reliance under section 1033.220(a)(6) is the natural route, which is one reason we regard the limitations on that provision as consequential. Our response to Question 7 develops this.
- Second, where the inbound transfer to the issuer redemption address originates from an institution, originator information transmitted under chapter X arrives with it. That data gives the issuer a verified starting point rather than a blank form. We recommend the agencies confirm that an issuer may treat originator information received under chapter X as part of the identifying information obtained under section 1033.220(a)(2)(i), while making clear it does not by itself satisfy the verification requirement in section 1033.220(a)(2)(ii).

Question 5

> *Should the regulatory text explicitly discuss digital identity solutions or verifiable credentials? How could it best do so given the range of tools available on the market?*

We support the agencies instinct to preserve flexibility, and we recommend one change in replacing silence with a short affirmative statement.

The reasoning is drawn from what we see when a rule declines to address a method. Compliance and examination teams read silence conservatively. A method the rule does not mention becomes a method the institution has to defend, and defending a method it did not have to use is a cost most institutions decline to bear. We watched this pattern play out with the Travel Rule. FinCEN guidance has applied to digital assets since 2019, and U.S. institutions still report widespread confusion about operational expectations, in large part because the requirements arrived by analogy rather than written for the asset class. The agencies noted in the preamble that guidance issued more than twenty years ago recognised an electronic credential as a route to a reasonable belief in identity. In our experience very few institutions know that guidance exists.

A short provision would resolve this without picking a technology. We suggest the substance be that an issuer may verify a customer identity using a digital identity credential or verifiable credential where the issuer risk-based procedures establish the assurance level of the credential and the basis for relying on it, and where the issuer makes a record under section 1033.220(a)(3). That formulation names the category, keeps the risk-based standard intact, and imports no technical specification into the Code of Federal Regulations.

Standards belong in guidance, where they can be updated. Two reference points are already in wide use and would give issuers something concrete to calibrate against. The identity

assurance levels in NIST Special Publication 800-63 are the common vocabulary among U.S. institutions for describing how strongly a credential is bound to a person. The FATF Guidance on Digital Identity provides the internationally recognised framing, which matters for issuers whose primary market counterparties are largely outside the United States. Neither should be mandated. Both would be useful as named reference points.

There is recent precedent for the approach we suggest. In its customer identification exemption order of July 31, 2025, FinCEN accepted that alternative verification processes are more prevalent than they once were and that, in some circumstances, those processes produce an equivalent or more reliable outcome than direct collection from the customer. The reasoning was applied to taxpayer identification numbers, and it supports a wider point. Where a method allows an institution to form a reasonable belief that it knows the true identity of a customer, the rule should not disadvantage it relative to a paper document simply because the rule was drafted around paper documents.

One drafting point on recordkeeping. Proposed section 1033.220(a)(3)(i)(B) asks for a description of any document relied on, with its type, identification number, place of issuance and dates of issuance and expiry. A verifiable credential does not decompose into those fields. We recommend the agencies confirm, in the text or in guidance, that a record describing the credential, its issuer, its assurance level, the verification method and the result satisfies this requirement. Without that confirmation the recordkeeping provision will quietly discourage the very methods the verification provision permits.

Question 6

> *What are the benefits and risks of using digital identity solutions or verifiable credentials as part of verifying customers' identities?*

Benefits

- Reusability: Reusability is the main one, and it connects directly to section 1033.220(a)(6). A credential issued once and verified many times is what makes reliance operational at scale rather than a bilateral negotiation repeated institution by institution.
- Data minimization: A well-designed credential proves a specific fact without transmitting the underlying document. Every avoided copy of a passport image is one fewer copy of a customer identity documents sitting in one more institution storage, which reduces the aggregate consequence of any single breach.
- Cryptographic binding raises the cost of forgery. A credential signed by its issuer and bound to the holder is materially harder to fabricate than a document image, which addresses synthetic identity and document fraud at the root rather than through detection.
- Machine readability lets the same verified attributes flow through onboarding, sanctions screening and transfer messaging without rekeying. Identity data entered

once and reused is more accurate than identity data entered four times, and the reduction in manual handling is itself a control.
- Audit quality improves. A verification event carrying a timestamp, a signature and a stated assurance level is a better record than a scanned image and a checkbox.

Risks

- Assurance level variation is the central one: Credentials that look alike differ enormously in how the underlying identity was proofed and how tightly the credential is bound to the person presenting it. An issuer accepting a credential without understanding its assurance level has not verified anything.
- Trust framework gaps compound this: In many schemes it is unclear who accredits credential issuers, what recourse a relying party has for a wrong assertion, and who bears the loss. Relying on a credential is relying on a party the issuer has no relationship with.
- Revocation and freshness are frequently underestimated: A credential valid at issuance may be revoked or superseded later, and a verifier needs a reliable and available way to check status at the moment of reliance.
- Presentation attacks are improving faster than defenses: Synthetic media and injection attacks against remote liveness and document capture are advancing quickly, and controls adequate in 2024 are not uniformly adequate now.
- Concentration risk grows with adoption: If a small number of credential providers become load bearing across the industry, an outage or compromise at one becomes a sector-wide event.
- Cross-border recognition is a live constraint for this population specifically. FinCEN's own analysis expects a substantial portion of primary market customers to be non-U.S. entities. Credentials issued under one national scheme are frequently not recognised under another, so a U.S. issuer serving foreign institutional counterparties will find the reusability benefit hardest to obtain where it would be worth the most.

A related technique worth recognising

A separate category of privacy-preserving verification is developing alongside credential-based identity, and it addresses a problem this rule will encounter directly.

Where two institutions each hold verified identity information on the same person, the objective is frequently not to move identity data between them but to confirm that both hold the same party. Cryptographic name matching achieves this. Rather than transmitting a name in the clear, the institutions exchange a hash of the normalised name. The receiving institution computes the same hash over the corresponding name in its own records and compares the values. A match confirms correspondence without either institution disclosing the underlying name to the other. Where the match fails, or the counterparty does not support the technique, the institutions fall back to full information exchange, so assurance is preserved.

The method is defined in an open standard contributed to the Transaction Authorization Protocol, so it interoperates across networks and providers rather than being confined to a single system. We recommended its recognition to the FATF in our response on Recommendation 16, and we recommend the agencies take the same approach here.

The relevance to this rule is specific. A permitted payment stablecoin issuer relying on another institution under section 1033.220(a)(6), or receiving a redemption instruction from a person already identified by an exchange, needs to establish that the person in front of it is the person the other institution verified. Confirming correspondence is a narrower operation than transferring an identity file, and it can be done without creating another copy of the customer identity data. We recommend the agencies confirm that privacy-preserving verification techniques of this kind (such as Cryptographic name matching) are a valid means of establishing correspondence, provided each institution continues to collect and retain the full required information and that information remains available to competent authorities.

Our recommendation across both categories follows the same pattern. Regulate at the assurance level rather than the tool level. The questions worth asking of any method are what it proves, at what assurance, bound to whom, and checkable by what means. Those questions remain answerable as the technology changes. A rule written around today tools would not.

Question 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?*

The demand for reliance is high. The uptake under the provision as drafted will be low. We think the gap is worth the agencies attention, because closing it is the change that would most reduce compliance cost in this rule without reducing any control.

Demand is high because of the market structure the agencies describe in their own analysis. Primary market participation is institutional. The truncated average issuer deals with roughly a thousand primary market customers, the median is one hundred, and the total population of U.S. business customers across all issuers is estimated at no more than ten thousand. Those customers are exchanges, trading firms, custodians and other financial institutions, and a large share already operate customer identification programs.

Uptake under the proposed reliance framework will be constrained by four specific structural limitations:

- The federal functional regulator condition excludes state qualified payment stablecoin issuers. The agencies acknowledge the resulting asymmetry, under which a state qualified issuer may rely on a subsidiary of an insured depository institution but not the reverse. In a market where charter choice is still being made, this creates a two-tier structure in which supervisory route determines commercial usefulness as a counterparty. The GENIUS Act already provides the answer through its certification mechanism for state regimes. Where a state regime has been certified as substantially

similar, the equivalence the federal functional regulator condition is testing for has been established through a different route. We recommend extending reliance to state qualified issuers supervised under a certified regime.

- There is no route for foreign financial institutions. FinCEN analysis states a substantial portion of primary market customers may be affiliates of a single counterparty or non-U.S. entities. As drafted, an issuer must perform full customer identification on a foreign exchange or custodian already subject to AML/CFT and customer identification obligations consistent with FATF standards, supervised for compliance at home, and frequently already exchanging identity data with U.S. counterparties under Recommendation 16. We recommend the agencies open a route, in the rule or through guidance, permitting reliance on a foreign financial institution subject to AML/CFT requirements consistent with FATF standards and supervised for compliance with them, retaining the contract and annual certification conditions. The European Union, United Kingdom, Singapore, United Arab Emirates and Japan each maintain explicit standalone frameworks that would support such a determination.
- Uncertainty over the reliance and outsourcing distinction will deter both. The preamble states clearly that engaging a third party to perform a service related to a customer identification program is not reliance, and that the obligation stays with the issuer. The regulatory text does not say this. In our experience institutions delay adopting shared compliance infrastructure precisely where supervisory expectations exist in preamble discussion rather than in rule text, because a preamble is a weaker answer to an examiner than a citation. We recommend section 1033.220(a)(6) state that engaging a third-party service provider to perform or support a customer identification procedure is not reliance for purposes of the paragraph, that the contract and annual certification conditions do not apply to such an arrangement, and that the issuer remains responsible for the procedure in all cases.
- A fourth point concerns the consequence of relying. The preamble states that reliance does not change the issuer obligation and that the issuer remains responsible for its compliance. Read strictly, that leaves open the possibility that an issuer is held responsible where a relied-upon institution fails to perform adequately, even where the issuer met every condition in the paragraph. Banks are not in that position. In the 2003 adopting release for the bank customer identification rule, the agencies stated that a bank will not be held responsible for the failure of another financial institution to fulfil the bank customer identification responsibilities, provided the bank establishes that its reliance was reasonable and that it obtained the requisite contracts and certifications, 68 Fed. Reg. 25,090, 25,104. We see no reason for a different rule here, and the difference will deter reliance on its own. We recommend the final rule adopt the same formulation.

We would add a point on what happens if reliance stays narrow, because the alternative is not a neutral outcome. Where an institution cannot rely on a counterparty and cannot establish an information-carrying connection to it, it does one of two things. It performs duplicative identification on the counterparty end customers, which is costly and produces no better

information than the counterparty already holds. Or it restructures the relationship bilaterally and treats the counterparty institution simply as its own customer, which simplifies the immediate relationship while obscuring who is actually on the other end of a transfer. We observe both across our network, and we raised the same concern with the FATF in our response on Recommendation 16. Neither improves identification, and both push the market toward closed structures and away from the interoperable networks that make transaction-level transparency possible. A workable reliance provision is the mechanism that prevents this.

One practical enabler is worth adding. Reliance functions where the relied-upon institution can hand over a structured, verifiable record rather than a document set assembled by hand. IVMS101 is already the international standard for identity attributes exchanged between institutions in digital asset transfers, and the same attributes underpin customer identification records. Transaction authorization protocols provide the complementary mechanism for identifying the institutions involved and coordinating the exchange. Encouraging interoperable formats in guidance would make reliance something institutions can operate at volume rather than negotiate one relationship at a time.

Question 8

> *What, if anything, could be changed to make the proposed rule more conducive to industry innovation? Explain how any changes would positively or negatively impact PPSIs expected operations and illicit finance risk to the U.S. financial system.*

We suggest five changes. Each asks the rule to recognise a control that works for this asset class, or to remove friction that produces cost without producing safety.

Recognise pre-transaction controls

Payment stablecoin settlement is irreversible, which inverts the usual relationship between monitoring and prevention. A control applied after settlement documents a loss. A control applied before settlement prevents one. Issuers and their counterparties increasingly operate on an authorize-then-settle basis, exchanging required originator and beneficiary information, screening both parties for sanctions exposure and verifying beneficiary details before on-chain finality. Within our network, participating institutions have blocked over $757 million in transfers where beneficiary details failed verification, and the share of institutions blocking withdrawals on failed verification continues to grow. We recommend the agencies confirm in examination guidance that pre-transaction identification and authorization controls of this kind, and reliance on specialized third-party compliance infrastructure to operate them, count as affirmative evidence of an effective program. The effect on illicit finance risk is to reduce it, because the controls stop transfers rather than reporting them.

Account for settlement addresses, and for the institution servicing them

We recommend the agencies confirm that a customer identification program should address, on a risk basis, the blockchain addresses a customer registers or allowlists with the issuer for settlement of mint and redeem instructions. Issuers already collect this information operationally, so the marginal cost is close to zero. The benefit is specific to this asset class and unavailable from a bank-style record. A customer identification file that links a verified identity to the on-chain identifiers that identity uses gives law enforcement a durable starting point, and gives the issuer a control it can apply at the moment of instruction rather than only at onboarding.

One qualification matters here, and we raised it with the FATF in the same terms. A blockchain address on its own is a weak identifier. Unlike an account number, it reveals neither the institution servicing the address nor the jurisdiction from which that service is provided. A record that captures the address alone therefore delivers less than it appears to. The useful record pairs the address with verifiable identification of the institution servicing it. Approaches now developing in the market, including decentralised identifiers used to identify a servicing institution alongside a user-level identifier, show how the combination can be achieved without requiring a traditional account number format. We do not suggest the agencies mandate any particular scheme, since adoption across the emerging approaches remains low. We suggest the rule be framed so it encourages movement toward identifiers that reveal the servicing institution and its jurisdiction, rather than entrenching the use of bare wallet addresses.

Recognise third-party infrastructure and interoperable standards

Carrying the reliance and outsourcing distinction into the regulatory text, as described in our response to Question 7, would remove the largest single deterrent to shared compliance infrastructure in this market. Encouraging structured, interoperable formats for identity attributes and authorization messaging, including IVMS101, makes customer identification outputs portable, which is what makes reliance work in practice. Interoperability across networks, protocols and data standards remains the principal barrier to scalable compliance in this sector, and regulatory frameworks that recognise the infrastructure category accelerate convergence rather than fragmentation.

Align recordkeeping

The five-year retention period in section 1033.220(a)(3) should be read alongside chapter X transaction recordkeeping so that an issuer maintains one record set on one retention clock rather than parallel sets with different triggers. Where the same identity attributes support both the customer identification record and the transaction record, the agencies should confirm a single record satisfies both.

Coordinate the effective date

As set out in our general comment above, we recommend the twelve month period run from the latest of the final FinCEN and OFAC rules, the final PPSI AML/CFT rule, the part 1033 framework and the parallel prudential rules, rather than from this rule alone.

We would add one observation on how innovation and illicit finance risk interact here. The instinct to treat them as a trade-off does not hold well for this asset class. The transparency of a public ledger, combined with structured identity data exchanged between institutions before settlement, makes it possible to build payment systems with better visibility than the correspondent chains they would replace. The rules that get this framework right are the ones that let institutions apply controls at the point where a transaction can still be stopped. That is where we would encourage the agencies to focus examination expectations as this framework takes effect.