WORLD FOUNDATION

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C23

Subject

Docket No. R-1885; RIN 7100-AH18 – World Foundation Comment – Permitted Payment Stablecoin Issuer Customer Identification Program

Submitter Information

Organization Name: World Foundation

Organization Type: Organization

Submitted Date: 08/21/2026

Hello,

Please find attached World Foundation's comments regarding the proposed rule, Permitted Payment Stablecoin Issuer Customer Identification Program, Docket No. R-1885; RIN 7100-AH18.

Best,
World Foundation

--
Dom Simon
Deputy GC
dominique.simon@world.org<mailto:dominique.simon@world.org>

WORLD FOUNDATION

August 21, 2026
Submitted electronically

Financial Crimes Enforcement Network, Department of the Treasury
Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration

Re: Permitted Payment Stablecoin Issuer Customer Identification Program

FinCEN Docket No. FINCEN-2026-0101; RIN 1506-AB74; OCC Docket No. OCC-2026-0331; RIN 1557-AF53; Board Docket No. R-1885; RIN 7100-AH18; FDIC RIN 3064-AG28; NCUA Docket No. NCUA-2026-0793; RIN 3133-AG09

World Foundation respectfully submits these comments on the joint proposal to establish customer identification program (CIP) requirements for permitted payment stablecoin issuers (PPSIs).[1] World Foundation is an independent nonprofit foundation focused on privacy-preserving digital infrastructure and public-interest approaches to digital identity, Proof of Human, and open digital systems.[2] For purposes of these comments, "Proof of Human" refers to a technology-neutral framework for describing different forms of assurance about the human behind a digital interaction, such as whether a human is participating, is uniquely represented within a defined system, is the same human established at an earlier event, or has approved a particular action. These forms of assurance are distinct from, and may supplement, proof of a person's legal identity.

The GENIUS Act requires PPSIs to maintain an effective CIP, including identification and verification of account holders. World Foundation supports that objective and the proposal's risk-based structure. The final rule should also preserve the distinction between direct customer relationships and secondary-market use, clearly protect non-custodial software and decentralized infrastructure, and provide practical recognition for trustworthy digital identity, verifiable credentials, and supplementary human-related assurance controls.[3]

Questions addressed. These comments respond to Questions 1, 2, 3, 5, 6, 7, and 8. World Foundation does not offer a view on Question 4.

I. Summary

1. **Preserve the direct-relationship boundary.** CIP should remain tied to an account established through a direct and formal relationship between a PPSI and a customer. Mere possession, receipt, or peer-to-peer transfer of a payment stablecoin through a self-hosted wallet should not create an issuer-customer relationship.
2. **Clarify the DASP definition around substantive intermediation.** The final rule should confirm that non-custodial software does not become a digital asset service provider merely because it constructs, signs, routes, transmits, or broadcasts a user-directed transaction without taking custody, exercising discretion, or controlling the assets.

[1] Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37,234 (June 22, 2026), https://www.federalregister.gov/documents/full_text/html/2026/06/22/2026-12460.html.
[2] foundation.world.org
[3] 12 U.S.C. § 5903(a)(5)(A)(v) (requiring maintenance of an effective customer identification program, including identification and verification of account holders).

3. **Recognize digital identity explicitly.** The final rule should expressly identify digital identity solutions, verifiable credentials, and cryptographically verifiable proofs, including zero-knowledge proofs, as permissible components of customer verification procedures.
4. **Distinguish identity proofing from human presence and human continuity.** Identity proofing uses evidence to establish who the customer is; CIP asks whether a PPSI can form a reasonable belief that it knows the customer's true identity. Human presence asks whether a human is actively present at the relevant interaction; human continuity asks whether the human at the current event corresponds to the human established at an earlier event. These controls address a separate remote-channel risk: even where reliable identity evidence exists, a PPSI may lack assurance that a live human is participating in the current interaction, rather than an automated process, replayed or synthetic-media artifact, or a different person using the customer's credential. Human presence can strengthen remote onboarding by confirming live participation, while human continuity can link a later, higher-risk action to the human established during onboarding. These controls may supplement, but do not replace, identity verification.
5. **Separate formal reliance from service-provider support.** Formal reliance under proposed § 1033.220(a)(6) should remain distinct from the use of third-party technology and credential providers as components of the PPSI's own CIP. In the latter model, the PPSI remains responsible.
6. **Promote data minimization and standards-based interoperability.** The agencies should permit auditable method-and-result records without requiring retention of raw biometric samples or media, and should coordinate with NIST and standards organizations on technology-neutral assurance terminology and conformance profiles.

Core recommendation: Adopt a technology-neutral approach that strengthens identity verification and recognizes and supports the use of supplementary human presence and human continuity controls where a regulated customer relationship exists, without turning downstream possession or peer-to-peer use of a lawful digital asset into a universal identification event.

II. CIP Should Remain Connected to a Direct and Formal Customer Relationship

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?*

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?*

Summary Response to Questions 1 and 3: Do not extend CIP to secondary-market activity. Retain "formal relationship," and provide examples centered on direct service, account-level dealings, and substantive intermediation—not mere token possession or protocol use.

World Foundation agrees with the proposal's decision to confine CIP to direct, primary-market relationships and not extend it to activity in which a user's only interaction with the PPSI is through a smart contract.[4] A person should not become the customer of an issuer merely by receiving, holding, or transferring a payment stablecoin that circulates on an open network.

[4] 91 Fed. Reg. at 37,238–41 (distinguishing primary-market relationships from secondary-market activity and limiting the proposed CIP definitions to direct relationships).

The proposal itself recognizes that imposing CIP across secondary-market activity would require PPSIs to identify a global and frequently pseudonymous population with whom the issuer has no direct relationship or practical channel for collecting information.[5] Such an approach would be operationally unworkable, would create incentives for unnecessary data aggregation, and could undermine the usefulness of self-hosted wallets and peer-to-peer payment functionality without reliably improving identity information available to the issuer.

Secondary-market risks should instead be addressed at appropriate regulated touchpoints. A digital asset exchange, custodian, money transmitter, or other regulated intermediary that establishes a customer relationship may have its own AML/CFT and identity obligations. A PPSI may separately apply sanctions controls, blockchain monitoring, transaction-risk measures, and lawful-order capabilities. Those controls should not be collapsed into a universal issuer-level CIP obligation for every downstream holder.

A. Retain "formal relationship," with functional examples

The final rule should retain "formal relationship" because it reflects the account-based structure of CIP and supplies an important limiting principle. Guidance should explain that relevant hallmarks may include:

- an account-opening process directly with the PPSI;
- ongoing access to services provided by the PPSI, rather than an isolated protocol interaction;
- customer-level records or credentials maintained by the PPSI;
- the PPSI's ability to limit, suspend, or terminate the customer's access to the relevant service; and
- direct provision of issuance, redemption, custody, or another authorized service to that person.

Conversely, the following should not, standing alone, establish a formal relationship: possession of a payment stablecoin; interaction with an open smart contract; use of non-custodial software; receipt of a transfer; connection of a wallet to a public interface; presentation of a privacy-preserving credential; or transmission of a user-directed transaction that the PPSI does not intermediate.

III. The DASP Definition Should Clearly Preserve Non-Custodial Software and Decentralized Infrastructure

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

Summary Response to Question 2: For purposes of proposed Part 1033, preserve the statutory exclusions and clarify that the DASP definition turns on substantive financial intermediation, custody, discretion, or control, not the technical capability of non-custodial software to facilitate a user-authorized transaction.

For purposes of proposed Part 1033, FinCEN and the Agencies propose a definition of digital asset service provider (DASP) based on the GENIUS Act, with technical modifications intended to align the definition with preexisting terminology in FinCEN's regulations. The statutory starting point covers specified business activities conducted for compensation or profit while expressly excluding distributed-ledger protocols, development or operation of self-custodial software interfaces, immutable self-custodial software interfaces, transaction validation, ledger operation, and peer-to-peer liquidity mechanisms.[6]

Those exclusions are essential and should be carried into the final rule without narrowing interpretation. World Foundation's requested clarification is limited to how the DASP definition operates in determining an

[5] Id. at 37,239, 37,258–59 (explaining that issuer-level identification of secondary-market users would be difficult or nearly impossible and noting that most stablecoin activity occurs in secondary markets).
[6] 12 U.S.C. § 5901(7); 91 Fed. Reg. at 37,240–41.

account or customer relationship under proposed Part 1033. In that context, the phrase “transferring digital assets to a third party” could be read too broadly if separated from the statutory requirements that the person act for compensation or profit and engage in the business of providing a financial service.

The final rule should clarify that a provider does not become a DASP merely because non-custodial software:

- generates, stores, or manages keys controlled by the user;
- constructs or displays a proposed transaction for user approval;
- signs a transaction using a user-controlled key or secure execution environment;
- routes, relays, transmits, or broadcasts a transaction selected and authorized by the user;
- displays balances or transaction history;
- connects a user to a distributed-ledger protocol or smart contract;
- allows a user to present a digital credential or cryptographic proof; or
- provides security, recovery, or interface functionality without taking custody or discretionary control of the assets.

The relevant inquiry should be functional: whether the business exercises custody, control, discretion, or substantive financial intermediation on behalf of the user. Technical facilitation of a user's own instruction should not be equated with acting as the financial intermediary that transfers the asset.

IV. Digital Identity and Verifiable Credentials Should Be Expressly Recognized

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?*

Question 6. *What are the benefits and risks of using digital identity solutions or verifiable credentials as part of verifying customers’ identities?*

Summary Response to Questions 5 and 6: The final rule should expressly recognize trustworthy digital identity tools, including verifiable credentials and other cryptographically verifiable proofs, without limiting PPSIs to those methods. These tools should be evaluated based on what they reliably establish and how well they perform, rather than the particular technology used. The rule should also recognize controls that confirm a live human is participating and, where relevant, that the participant is the same person previously verified. Those controls can strengthen, but do not replace, verification of the customer’s identity.

The proposal recognizes that digital identity and verifiable credentials can serve as documentary or non-documentary verification methods, but does not include them in the proposed regulatory text.[7] World Foundation recommends a short, non-exclusive reference in the rule, supported by functional criteria in the guidance.

That clarification would implement—not depart from—Treasury's March 2026 findings. Treasury identified verifiable credentials as a means of conducting customer identification while reducing collection of sensitive data and adopted recommendations to issue CIP guidance, promote interoperable guidelines, and enable trusted third parties to conduct identity verification and issue credentials.[8]

[7] 91 Fed. Reg. at 37,242–43 (recognizing mobile IDs, digital identity credentials, and verifiable credentials as potential documentary or non-documentary methods while declining to include specific regulatory text).
[8] U.S. Department of the Treasury, Report to Congress on Innovative Technologies to Counter Illicit Finance Involving Digital Assets 17–22 (Mar. 2026), https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.

A. Permit PPSIs to combine identity services from different providers

A PPSI should not be expected to rely on a single provider to perform every part of identity verification. One provider may validate identity evidence, another may issue a verifiable credential, a wallet may protect the relevant key, and another provider may verify the credential when it is presented. Separate services may also confirm that a human is presently participating or that the participant is the same human previously verified.

A PPSI should be permitted to combine these services, while remaining responsible for determining whether the overall process enables it to form a reasonable belief that it knows the customer's true identity. Separating these functions can improve security and privacy because each provider can receive and retain only the information necessary to perform its particular role. The final rule should avoid an implicit expectation that one credential provider must collect every CIP field, perform original identity proofing, protect the holder's key, establish human presence or continuity, verify corporate authority, conduct sanctions screening, and retain all records.

B. Use functional, technology-neutral evaluation criteria

The agencies should not endorse a particular provider, credential format, biometric technology, or technical architecture. A PPSI should instead evaluate a digital identity method based on factors such as:

- the reliability of the information or evidence on which it is based;
- who issued the credential or proof and how trustworthy that issuer is;
- what the credential or proof actually establishes;
- whether it is current, valid, and resistant to theft, replay, or manipulation;
- its security, privacy, and data-retention characteristics; and
- its demonstrated performance and availability of appropriate recovery or alternative methods.

C. Recognize human presence and human continuity as supplementary controls

Remote identity verification creates a separate problem from establishing who the customer is. A PPSI may have reliable identity information but still need confidence that a live human is participating in the current interaction, rather than an automated process, replayed or synthetic image or video, or another person using the customer's credentials.[9]

Human presence and human continuity address different assurance questions. Human presence assurance asks whether a real human is actively participating in a particular interaction at that time. It does not establish who that human is. Human continuity assurance asks whether the human participating in the current interaction is the same human established at a specified earlier event, such as the customer's original identity verification. It therefore links the human at two different events without requiring the PPSI to repeat the full identity-proofing process.

These concepts are also distinct from control of a credential, account, device, or authenticator. Possession or control may show that the presenter has access to the relevant credential, but does not necessarily establish that the person using it is the human whose identity was originally verified. Human continuity can therefore provide additional assurance against risks such as credential sharing, account takeover, impersonation, or substitution of another person.

These assurances may be supported by biometric or non-biometric evidence. Depending on the method and risk, relevant evidence may include liveness or presentation-attack detection, fresh user challenges, credential control, session or device signals, and binding the verification to a particular transaction or

[9] FinCEN, Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions, FIN-2024-Alert004 (Nov. 13, 2024), https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial.

interaction. The appropriate evidence should reflect threats such as replay, synthetic media, injection, relay, or session handoff.

The regulatory role of these controls is supplementary. They can strengthen confidence that the relevant human is present and, where needed, is the customer previously verified, while CIP's core objective remains forming a reasonable belief that the PPSI knows the customer's true identity. The final rule should recognize their risk-based use in remote onboarding and as step-up controls for account recovery, material account changes, redemptions, changes to settlement instructions, or other higher-risk actions.

D. Benefits and risks

Digital identity tools and verifiable credentials can improve customer verification in several ways. They can allow a PPSI to verify information directly from a trusted source, reduce repeated collection and storage of identity documents, support selective disclosure of only the information needed for a particular purpose, and make credentials easier to validate, update, or revoke. When appropriately designed and bound to the customer, they may also reduce certain forms of document fraud and make it easier to establish that the information presented during a remote interaction is authentic.

Those benefits depend on the quality of the underlying process. A digitally verifiable credential is only as reliable as the identity proofing or other evidence on which it is based. Credentials may also be stolen, transferred, shared, or presented by someone other than the person to whom they were issued. Other risks include excessive tracking or correlation across services, concentration in a small number of providers, inaccessible recovery processes, exclusion of users who cannot use a particular technology, and inaccurate or biased performance where biometric systems are used.

The final rule should therefore avoid treating any particular credential or technology as inherently sufficient. PPSIs should evaluate what a digital credential or proof actually establishes, how reliably it establishes it, and whether additional controls are appropriate for the particular interaction. Human presence and human continuity controls may address some risks concerning who is participating at the time of use, but they do not cure weak underlying identity proofing and should not be treated as substitutes for it.

V. Formal Reliance and Third-Party Service Support Should Be Clearly Distinguished

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?*

Summary Response to Question 7: Retain the narrow formal-reliance mechanism, but expressly confirm that PPSIs may use qualified third-party digital identity and assurance services within their own CIP while retaining legal and supervisory responsibility.

World Foundation is not positioned to quantify how often PPSIs will use the proposed formal-reliance provision. Formal reliance is likely to be most useful in institutional primary-market relationships, enterprise structures, and arrangements involving banks or other federally regulated financial institutions that can satisfy the proposed contract and annual-certification requirements.

Use of third-party technology and credential services is likely to be more common than formal reliance. The proposal correctly states that the restrictions on reliance should not prevent third parties from performing services related to a PPSI's CIP, provided the obligation remains with the PPSI.[10]

The final rule should expressly distinguish:

Formal reliance. The PPSI relies on a qualifying federally regulated financial institution to perform a specified CIP procedure under the conditions in proposed § 1033.220(a)(6).

Service-provider support. A provider supplies identity evidence, credential issuance or validation, human presence or human continuity controls, fraud signals, or verification functionality as part of the PPSI's own risk-based CIP. The PPSI remains responsible.

For service-provider arrangements, PPSIs should apply due diligence and appropriate contractual controls concerning security, privacy, audit rights, incident notification, continuity, subcontractors, model or performance changes, credential status, termination, and access to records. A credential issued by a non-financial institution may be relevant evidence without converting the arrangement into statutory reliance.

VI. Targeted Changes Would Support Responsible Innovation Without Weakening CIP

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.*

Summary Response to Question 8: Clarify data-minimizing records; encourage common assurance terminology and conformance profiles; and use coordinated guidance and pilots to support responsible adoption without weakening PPSI accountability or expanding CIP beyond direct customer relationships.

A. Clarify data-minimizing recordkeeping

The final rule should permit a PPSI to satisfy the method-and-result portion of its recordkeeping obligation through structured verification metadata, where appropriate. That metadata could include the assurance category or categories claimed, required strength, evidence or method class, credential issuer or trust framework, relevant context and freshness, validity or revocation result, session, reference-event or transaction binding, outcome, and resolution of substantive discrepancies.

The agencies should also clarify that the CIP rule does not itself require retention of raw biometric samples, biometric templates, video, facial images, or a complete copy of every underlying identity document where the PPSI retains the required identifying information and sufficient records describing the method and result. Mandatory retention of high-risk source material would increase breach consequences and could deter adoption of privacy-preserving methods without providing a commensurate supervisory benefit.

B. Develop a common assurance taxonomy for Proof of Human and conformance profiles

NIST SP 800-63-4 provides a mature framework for identity proofing, authentication, and federation.[11] W3C Verifiable Credentials 2.0 provides an interoperable data model for issuer-holder-verifier credentials and presentations.[12]

Existing ISO work separately addresses identity proofing, biometric presentation-attack testing, and privacy-preserving use of zero-knowledge proofs. These standards provide important evidence, evaluation,

[10] 91 Fed. Reg. at 37,243–44 (distinguishing formal reliance from appropriate use of third parties to perform services on the PPSI's behalf, with responsibility remaining with the PPSI).
[11] NIST, Special Publication 800-63-4, Digital Identity Guidelines (July 2025), https://csrc.nist.gov/pubs/sp/800/63/4/final.
[12] W3C, Verifiable Credentials Data Model v2.0, W3C Recommendation (May 15, 2025), https://www.w3.org/TR/vc-data-model-2.0/.

and privacy building blocks. A common Proof of Human assurance taxonomy can complement them by providing consistent semantics for the assurance outcome being claimed, the strength required, the evidence supporting it, and the context in which it applies.[13]

The GENIUS Act separately directs the primary federal payment stablecoin regulators, in consultation with NIST and other standard-setting organizations, to assess and, if necessary, prescribe interoperability standards.[14] The CIP rule should use that mandate to promote consistent terminology and conformance profiles without selecting a particular provider or implementation architecture.

A standards-oriented Proof of Human taxonomy should distinguish the following assurance categories. CIP directly concerns identity assurance; other categories may supplement CIP or support related higher-risk controls without altering the rule's core requirement that a PPSI form a reasonable belief that it knows the customer's true identity.

Assurance category	Core question
Identity assurance	Which person is this in legal or civil terms?
Humanity assurance	Is the subject a human being?
Uniqueness assurance	Is this one distinct human within a defined domain?
Credential control assurance	Does the presenter control the relevant credential, authenticator, or key?
Human presence assurance	Is a human actively present in the relevant interaction or event now?
Human continuity assurance	Is the human at this event the same human established at a specified earlier assurance event?
Attribute assurance	Does the human possess a defined characteristic or eligibility fact?
Role assurance	Does the human hold a defined role, relationship, or mandate?
Action assurance	Did the human approve this defined action?
Agent authority assurance	What authority has a human or organizational principal delegated to this agent?

C. Use guidance, pilots, and coordinated supervision

The agencies can reduce uncertainty without freezing technology through interagency FAQs, illustrative use cases, supervised pilots, model risk and testing expectations, and a technical profile developed with NIST and relevant standards bodies. The final rule should make clear that the regulatory objective remains a reasonable belief in the customer's true identity supported by evidence appropriate to the risk—not adoption of any particular credential format, biometric modality, or single liveness mechanism.

[13] See ISO/IEC TS 29003:2018, Identity Proofing, https://www.iso.org/standard/62290.html; ISO/IEC 30107-3:2023, Biometric Presentation Attack Detection—Testing and Reporting, https://www.iso.org/standard/79520.html; ISO/IEC 27565:2026, Guidelines on Privacy Preservation Based on Zero-Knowledge Proofs, https://www.iso.org/standard/80398.html.
[14] 12 U.S.C. § 5912 (directing the primary Federal payment stablecoin regulators, in consultation with NIST and other relevant standard-setting organizations, to assess and, if necessary, prescribe interoperability standards).

VII. Conclusion

World Foundation is committed to the development of privacy-preserving digital infrastructure and practical approaches to digital identity and human assurance. We believe that privacy-preserving and technology-neutral principles are critical to support a strong and effective CIP framework for PPSIs while reducing unnecessary collection of sensitive information and preserving responsible innovation. We hope that the observations and recommendations in these comments will assist the Agencies as they develop the final rule.

We appreciate the opportunity to provide comments on these important issues and look forward to continued engagement with the Agencies.