

August 18, 2026

Financial Crimes Enforcement Network
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

91 Fed. Reg. 37234 (June 22, 2026)
FinCEN Docket FINCEN-2026-0101 | RIN 1506-AB74
OCC Docket OCC-2026-0331 | RIN 1557-AF53
Federal Reserve Docket R-1885 | RIN 7100-AH18
FDIC RIN 3064-AG28
NCUA Docket NCUA-2026-0793 | RIN 3133-AG09

Comment on Permitted Payment Stablecoin Issuer Customer Identification Program

To the Agencies:

TauriPay Public Benefit Corporation respectfully submits this comment in response to the joint proposed rule concerning Customer Identification Program (“CIP”) requirements for permitted payment stablecoin issuers (“PPSIs”).

The proposed rule implements provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (“GENIUS Act”) directing that PPSIs be treated as financial institutions for purposes of the Bank Secrecy Act (“BSA”) and requiring PPSIs to maintain an effective customer identification program, including identification and verification of the identity of account holders.¹

TauriPay supports the Agencies’ objective of establishing an effective, consistent, and technology-neutral customer identification framework for PPSIs.

Our principal observation is straightforward:

Identity, customer relationship, authority to act, and technical interaction are related concepts, but they are not interchangeable.

A person or legal entity may hold or transfer a payment stablecoin without maintaining a direct relationship with its issuer. A properly identified institutional customer may authorize individuals, systems, wallets, cryptographic keys, or automated or agentic systems to act on its behalf. Another regulated financial institution may already have performed customer identification upon which a PPSI reasonably relies. Emerging digital identity technologies may also permit an identity fact to be reliably verified without requiring every participant in a financial workflow to maintain another complete copy of the underlying sensitive information.

The particular architecture may vary substantially. These functions may be administered within a single regulated institution or distributed among multiple institutions, systems, and service providers. The regulatory framework should not presume a particular technical architecture.

The final framework should recognize these distinctions while preserving clear responsibility and supervisory accountability.

¹ Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37234, 37235-36 (June 22, 2026) (joint proposed rule); see also 12 U.S.C. § 5903(a)(5)(A), (a)(5)(A)(v); 31 U.S.C. § 5318(l).

TauriPay therefore recommends that the Agencies:

- I. Preserve a clear distinction between a substantive PPSI customer relationship and secondary-market ownership or transfer of the payment stablecoin;
- II. Clarify when a “formal relationship” with a PPSI begins;
- III. Avoid conflating successful customer identification with authority to act for the identified customer;
- IV. Maintain a technology-neutral approach to digital identity and verifiable credentials while preserving appropriate evidentiary standards;
- V. Facilitate appropriate reliance on customer identification performed by other qualifying regulated financial institutions without reducing accountability;
- VI. Permit privacy-preserving verification approaches that reduce unnecessary replication of sensitive customer information while preserving appropriate records and lawful supervisory access; and
- VII. Preserve risk-based flexibility in how PPSIs satisfy CIP requirements without weakening the core identification standard.

These recommendations respond principally to Questions 1 through 8 posed by the Agencies.²

I. CIP Should Attach to the Direct Issuer Relationship, Not the Circulation of the Instrument

Response to Questions 1 and 4

TauriPay supports the Agencies’ proposed distinction between primary- and secondary-market activity.

That distinction is important not only for determining when CIP applies, but also for preserving the ability of a payment stablecoin to circulate without converting every subsequent holder into a customer of the issuer.

The NPRM describes the primary market as activity in which the PPSI interacts directly with a user or holder, including issuance, conversion, redemption, repurchase, burning, reissuance, and associated services such as custody. It describes the secondary market as activity that does not directly involve the PPSI as a party other than through a smart contract. Examples include person-to-person transactions, purchases from intermediaries, payments from self-hosted wallets to vendors, and exchanges of stablecoins for other digital assets.³

This distinction reflects the way stablecoins may circulate in practice. The Agencies observe that many issuers currently interact directly with a relatively small number of larger institutional participants, which in turn place stablecoins into broader circulation among other users.⁴

The proposed regulatory text similarly defines an “account” as a formal relationship between a customer and PPSI established to provide or engage in services, dealings, or other financial transactions, including issuance or redemption. The definition excludes payment-stablecoin activity that does not directly involve the PPSI other than through a smart contract and excludes ownership or control of the PPSI’s payment stablecoin alone, without other indicators of a formal relationship.⁵

Once issued, a payment stablecoin may therefore move among individuals, businesses, wallets, intermediaries, trading venues, applications, and other participants without the PPSI establishing a direct relationship with every subsequent holder.

TauriPay does not recommend extending the PPSI’s CIP obligation generally to such secondary-market activity where no direct customer relationship with the PPSI has been established.

Ownership, receipt, payment, or transfer of the instrument should not, by itself, establish a CIP customer relationship with the issuer.

Otherwise, the regulatory framework would blur an important distinction between identifying the issuer’s customer and identifying every subsequent holder of an instrument issued by that institution.

² 91 Fed. Reg. at 37244 (Questions 1-8).

³ Id. at 37238 (describing primary- and secondary-market activity and providing examples of secondary-market transactions).

⁴ Id. at 37238 (describing current issuer interactions with institutional participants and subsequent broader circulation).

⁵ Proposed 31 C.F.R. § 1033.100(a), 91 Fed. Reg. at 37239-40, 37270.

The boundary should operate consistently in both directions.

A person or legal entity establishing a direct issuance relationship with a PPSI enters the type of direct issuer relationship contemplated by the proposed account definition and should be subject to the applicable CIP. Likewise, a person or legal entity that acquired payment stablecoins elsewhere and subsequently establishes a direct redemption relationship with the PPSI should be treated as a customer at that point.

Activity occurring between those direct relationships should not, merely because the PPSI's stablecoin is involved, create a new CIP relationship with the issuer.

This approach is consistent with the proposed definition of "customer," which excludes a person acquiring or redeeming a payment stablecoin other than directly from or directly to the PPSI.⁶

Direct Redemption

A person or legal entity may acquire a payment stablecoin through secondary-market activity and subsequently approach the PPSI directly for redemption.

TauriPay believes the regulatory boundary should remain clear.

Secondary-market ownership, receipt, payment, or transfer alone should not establish a CIP customer relationship with the PPSI. When a holder establishes a direct redemption relationship with the PPSI, however, that interaction establishes the customer relationship to which the PPSI's CIP applies.

A holder seeking to redeem directly with the PPSI should do so through an existing customer relationship or establish the required customer relationship and complete the applicable customer identification and verification process before redemption. The relevant CIP question is who the customer seeking redemption is, not how that customer originally acquired the stablecoin.

This distinction would allow payment stablecoins to circulate through secondary-market activity without treating every subsequent holder as a customer of the issuer, while ensuring that persons or legal entities that establish direct issuance or redemption relationships with the PPSI are subject to the issuer's applicable customer-identification procedures.

The Agencies expressly request comment on whether the proposed rule should be clarified or refined where a customer's only desired relationship with a PPSI is redemption. TauriPay recommends that any such clarification preserve this direct-relationship boundary.⁷

II. "Formal Relationship" Should Be Defined by the Substantive Relationship, Not the Technical Pathway

Response to Questions 2 and 3

The proposed rule defines an "account" as a "formal relationship" between the customer and PPSI established to provide or engage in services, dealings, or other financial transactions. The Agencies specifically request comment on whether "formal relationship" is sufficiently clear, what its hallmarks should be, and whether concepts such as a contractual or business relationship could provide a better foundation.⁸

Distributed financial infrastructure can separate the substantive financial relationship from the technical pathway through which an instruction is delivered.

A wallet may interact with a smart contract. One smart contract may invoke another. An intermediary may aggregate activity on behalf of multiple customers. Automated or agentic systems may construct, route, or submit instructions to issuer-supported infrastructure.

Those technical interactions do not necessarily establish a new underlying financial relationship.

TauriPay therefore recommends that the existence of a "formal relationship" be determined principally by the substantive financial relationship established between the PPSI and the person or legal entity, rather than

⁶Id. at 37238 (describing current issuer interactions with institutional participants and subsequent broader circulation).

⁷Proposed 31 C.F.R. § 1033.100(a), 91 Fed. Reg. at 37239-40, 37270.

⁸Proposed 31 C.F.R. § 1033.100(b), 91 Fed. Reg. at 37240, 37270.

solely by whether a wallet, application, automated system, agentic system, or smart contract technically interacts with issuer-supported infrastructure.

Relevant indicators could include:

- a contractual or business relationship with the PPSI;
- establishment of an issuer-maintained account;
- direct issuance or redemption arrangements;
- custody or safeguarding services;
- issuer-administered account permissions associated with an established financial relationship; or
- another arrangement under which the PPSI undertakes continuing obligations directly to the person or legal entity.

The principle is straightforward:

The technical route by which an instruction reaches infrastructure should not, standing alone, determine the regulatory character of the underlying customer relationship.

Digital Asset Service Providers and Underlying Infrastructure

The same distinction is relevant to the proposed definition of “digital asset service provider.”

The proposed regulatory text defines certain compensated or for-profit digital-asset financial services as digital asset service provider activities while expressly excluding, among other things, distributed-ledger protocols, development or operation of distributed-ledger protocols or self-custodial software interfaces, validation or operation of a distributed ledger, and certain peer-to-peer liquidity mechanisms.⁹

TauriPay supports maintaining this distinction.

The final framework should distinguish between a person or entity providing a substantive financial service to a customer and the underlying infrastructure through which an instruction is processed, validated, or transmitted.

A distributed-ledger protocol, validator or other network operator, self-custodial software, or automated technical system can perform important functions without necessarily establishing the customer-facing financial relationship to which CIP should attach.

The relevant CIP inquiry should therefore remain focused on the person or legal entity establishing the substantive financial relationship rather than treating underlying transaction infrastructure itself as a customer-facing service provider merely because it processes, validates, or transmits an instruction.

This preserves regulatory accountability while avoiding the conflation of financial relationships with infrastructure functions.

III. Customer Identity Should Not Be Conflated With Authority to Act for the Customer

Response principally to Questions 2 and 3

Customer identification answers the threshold CIP question:

Who is the customer?

The proposed rule requires risk-based procedures that enable the PPSI to form a reasonable belief that it knows the true identity of each customer.¹⁰

For certain non-individual customers, the proposal also recognizes that information concerning individuals with authority or control over an account may become relevant where the PPSI cannot otherwise verify the customer’s true identity.¹¹

That illustrates an important distinction.

In institutional relationships, identifying the customer and determining whether a particular person or mechanism is authorized to act for that customer are related, but separate, questions.

⁹91 Fed. Reg. at 37240, 37244 (Question 4).

¹⁰Id. at 37239, 37244 (discussion of “formal relationship” and Questions 2-3).

¹¹Proposed 31 C.F.R. § 1033.100(c), 91 Fed. Reg. at 37240-41, 37270.

An institutional customer may be fully identified under a compliant CIP without that determination, by itself, establishing whether a particular employee, agent, wallet, cryptographic key, automated system, or agentic system is authorized to act for the customer.

An instruction may, for example, be constructed or presented by an automated or agentic system acting on behalf of an identified customer. Use of such a system should not, by itself, alter the identity of the underlying customer or make the system independently a customer. The relevant questions remain who established the substantive relationship with the PPSI and, separately, whether the person or mechanism presenting an instruction is authorized to act for that customer.

The particular architecture may vary. Identity, signing authority, account permissions, custody, and transaction execution may be administered within a single regulated institution or distributed among multiple systems and service providers.

TauriPay does not recommend expanding CIP to regulate wallet control, transaction entitlements, cryptographic authorization, agentic authorization, or other transaction-level permissions.

The narrower point is that successful identification of the customer should not itself be treated as establishing those separate facts.

Maintaining that conceptual boundary will preserve the scope of CIP while reducing ambiguity as institutional payment-stablecoin architectures develop.

IV. Digital Identity Should Remain Technology-Neutral but Evidence-Based and Auditable

Response to Questions 5 and 6

The Agencies specifically request comment on whether the regulatory text should address digital identity solutions or verifiable credentials and on the benefits and risks of using such technologies to verify customer identity.¹²

TauriPay supports a technology-neutral approach.

Digital identity mechanisms may reduce duplicative identification processes, improve interoperability, support automation, and reduce unnecessary dissemination of sensitive personal information.

The regulatory framework should not prescribe a particular credential technology or architecture.

At the same time, flexibility regarding technology should not reduce the quality of evidence supporting an identity determination.

The proposed rule already requires a PPSI's CIP to address documentary and non-documentary verification. It also would require records of identifying information, descriptions of documents relied upon, descriptions of methods and results of verification measures, and resolution of substantive discrepancies.¹³

Where digital credentials are used as part of a non-documentary verification process, TauriPay recommends that the Agencies consider whether guidance should identify evidentiary characteristics relevant to evaluating such credentials.

Depending upon the credential and use case, those characteristics could include:

- who issued or attested to the credential;
- what identity attributes were verified;
- the methodology used to perform that verification;
- when verification occurred;
- the assurance represented by the credential;
- whether the credential remains valid;
- expiration, revocation, status change, or another loss of validity, as applicable; and
- whether sufficient evidence exists to reconstruct the basis for reliance during examination or investigation.

These characteristics should not be interpreted as requiring every credential to contain every data element or as establishing a standardized credential format.

Different credential and verification architectures may establish the necessary evidence in different ways.

¹²Proposed 31 C.F.R. § 1033.220(a)(2), 91 Fed. Reg. at 37241, 37271.

¹³Proposed 31 C.F.R. § 1033.220(a)(2)(ii)(C), 91 Fed. Reg. at 37242, 37271-72.

For clarity, provenance in this context means the provenance of the identity evidence, credential, assertion, or proof being relied upon. It does not mean the transactional provenance of the payment stablecoin.

The supervisory objective should remain focused on the quality, provenance, persistence, and auditability of the evidence supporting the identity determination, rather than the technological format in which that evidence is represented.

V. Reliance on Other Regulated Financial Institutions Should Reduce Duplication Without Reducing Accountability

Response to Question 7

The proposed rule permits a PPSI, under specified conditions, to rely upon another Federally regulated financial institution's performance of a CIP procedure for a PPSI customer.

Such reliance must be reasonable under the circumstances. The other financial institution must be subject to an AML/CFT program with CIP requirements and regulated by a Federal functional regulator, and the institutions must maintain a contractual arrangement under which the relied-upon institution annually certifies specified matters. The proposal nevertheless preserves the PPSI's responsibility for its own CIP compliance.¹⁴

TauriPay supports this approach. TauriPay expects such reliance to be meaningful in institutional payment-stablecoin arrangements, particularly where PPSIs interact with banks, custodians, trading venues, payment providers, or other regulated financial institutions that already maintain CIPs.

Institutional payment-stablecoin activity may involve banks, custodians, trading venues, payment providers, and other regulated financial institutions that already maintain customer identification programs.

Requiring every institution participating in a financial workflow to independently recreate the same identity file may increase cost and expand the number of locations in which sensitive customer information is stored without necessarily improving the quality of customer identification.

As implementation develops, the Agencies should consider whether additional guidance is warranted concerning the evidence supporting institutional reliance in digitally interoperable environments.

These observations are not intended to modify the conditions under which reliance is legally permissible. They address how permissible reliance can remain operationally traceable when identity assertions or proofs are presented, verified, or exchanged through interoperable systems.

Where a PPSI relies upon another regulated institution, sufficient evidence should permit the PPSI and its supervisor, as appropriate, to determine:

- which institution performed the identification;
- what identity determination, assertion, or proof is being relied upon;
- when the relevant verification occurred;
- the basis for the PPSI's reliance;
- where the supporting identity-verification evidence is maintained and how it can be made available when required;
- how expiration, revocation, status changes, or other material changes in validity are communicated, as applicable; and
- how the chain of reliance can be reconstructed when necessary.

Interoperability should not make responsibility ambiguous. At each point of reliance, the regulated institution should be able to identify the party responsible for the underlying identity determination and where the supporting identity evidence is maintained.

Reliance should also remain conceptually distinct from outsourcing.

The NPRM recognizes that the limitations on reliance do not prohibit appropriate use of third parties to perform CIP-related services on the PPSI's behalf, while the CIP obligation remains with the PPSI.¹⁵

¹⁴91 Fed. Reg. at 37244 (Questions 5-6).

¹⁵Proposed 31 C.F.R. § 1033.220(a)(2)(ii), (a)(3), 91 Fed. Reg. at 37242-43, 37271-72.

A PPSI's reliance upon another qualifying regulated financial institution's CIP is therefore not necessarily the same arrangement as engaging a third-party service provider to perform a CIP-related function.

Distributed infrastructure may make it technically easier to present, verify, or exchange an identity assertion or proof between institutions than to transfer the underlying customer file.

That capability can improve efficiency, but it should not obscure responsibility for the underlying identity determination.

Reliance should reduce duplicative collection without reducing accountability.

VI. Privacy-Preserving Verification Can Promote Innovation Without Weakening CIP

Response to Question 8 and related Questions 5 and 6

The Agencies ask what changes could make the proposed rule more conducive to industry innovation and how such changes could affect PPSI operations and illicit-finance risk.¹⁶

One appropriate avenue is to permit risk-appropriate use of privacy-preserving, machine-verifiable identity assertions or proofs.

Customer identification and customer-data replication should not automatically be treated as the same regulatory objective.

A PPSI must be able to establish the identity of its customer and maintain the evidence required by the applicable CIP framework.

That does not necessarily require every institution or technical participant in a financial workflow to maintain another complete copy of the customer's underlying identity documents.

Digital credentials and related technologies may allow institutions or customers to present and verify specific required facts while limiting unnecessary disclosure of unrelated information.

A properly structured framework could reduce unnecessary replication of sensitive information while preserving:

- reliable verification;
- provenance of the relevant identity assertion or proof;
- clear responsibility for the underlying identity determination;
- appropriate record retention;
- applicable validity and status mechanisms;
- auditability; and
- lawful supervisory and investigative access.

Privacy-preserving approaches should also seek to avoid unnecessary correlation of a customer's activity across otherwise unrelated services while retaining the records necessary for lawful supervisory and investigative purposes. Properly implemented, these approaches should not reduce the identification standard or the evidence available for lawful supervisory and investigative purposes and therefore need not increase illicit-finance risk merely because less underlying customer data is replicated across participants.

This could reduce cybersecurity and privacy exposure associated with unnecessary copies or dissemination of sensitive identity information while supporting interoperability among regulated institutions.

The Agencies' Paperwork Reduction Act discussion separately requests comment on ways to enhance the quality, utility, and clarity of required information and ways to minimize collection burden through automated collection techniques or other forms of information technology. Appropriate digital-verification architectures may further those objectives.¹⁷

Privacy preservation and supervisory accountability therefore need not be competing objectives.

The relevant question is whether the verification architecture preserves the evidence and responsibility necessary to satisfy the regulatory objective.

¹⁶Proposed 31 C.F.R. § 1033.220(a)(6), 91 Fed. Reg. at 37243, 37273.

¹⁷91 Fed. Reg. at 37243-44.

VII. Risk-Based Flexibility Should Preserve the Core Identification Standard

The GENIUS Act directs Treasury to tailor implementing BSA regulations to the size and complexity of the PPSI. The Agencies explain that the proposal implements this direction by requiring a PPSI to tailor its CIP to its size and business and by requiring risk-based verification procedures that take account of the PPSI's particular circumstances.¹⁸

The proposed regulatory text accordingly requires a written CIP appropriate for the PPSI's size and business. Its identity-verification procedures must be risk-based, reasonable, and practicable and must enable the PPSI to form a reasonable belief that it knows the true identity of each customer.¹⁹

TauriPay supports this approach.

PPSIs may range from relatively straightforward issuance models to institutional platforms involving multiple account types, intermediaries, credential mechanisms, and methods of interaction.

The method by which an appropriate CIP is implemented may therefore differ.

But flexibility should affect how a PPSI satisfies the customer-identification requirement, not eliminate the underlying objective.

Risk-based procedures should still enable the PPSI to form the reasonable belief concerning customer identity required by the CIP framework.

Likewise, the emergence of a new technical architecture should not itself justify a lower evidentiary standard.

Instead, the framework should permit different technical means of satisfying a consistent regulatory objective.

That balance, flexibility in implementation coupled with clarity of responsibility, can accommodate innovation without weakening customer identification.

¹⁸Id. at 37244 (Question 8).

¹⁹Id. at 37268 (Paperwork Reduction Act request for comment).

Conclusion

TauriPay supports the Agencies' effort to establish a consistent Customer Identification Program framework for permitted payment stablecoin issuers.

We recommend that the final framework preserve the distinction between direct issuer relationships and secondary-market ownership; clarify when a formal issuer relationship begins; avoid conflating customer identity with authority to act for the customer; permit technology-neutral digital identity mechanisms subject to meaningful evidentiary standards; facilitate auditable reliance among regulated institutions; permit privacy-preserving verification without reducing supervisory accountability; and preserve risk-based flexibility in implementation without weakening the core customer-identification standard.

A durable CIP framework should allow a payment stablecoin to circulate without making every subsequent holder a customer of the issuer, while establishing a clear customer-identification obligation when a person or legal entity enters into the direct issuer relationship to which CIP applies.

There is a broader operational reason these distinctions matter.

In conventional account-based infrastructure, customer identity, account permissions, transaction authority, recordkeeping, and the authoritative ledger may often be administered within the same institutional environment.

Distributed financial infrastructure can separate those functions among issuers, custodians, intermediaries, wallets, smart contracts, credential providers, automated or agentic systems, and transaction networks.

Alternatively, many or all of those functions may remain within a single regulated institution.

The regulatory framework need not prescribe either architecture.

But where functions are separated, that separation does not diminish regulatory responsibility.

It makes clear allocation of responsibility and evidence more important.

The objective of customer identification should therefore remain consistent even where the infrastructure through which that objective is implemented changes.

A durable framework should establish clear responsibility for knowing the customer while remaining sufficiently precise about how identity, relationship, authority, evidence, and accountability operate across different systems and participants.

Respectfully submitted,

Mark Sulavka

TauriPay, a Public Benefit Corporation