INHERENCE, INC., JING JIAN

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C19

Submitter Information

Organization Name: Inherence, Inc.

Organization Type: Company

Name: Jing Jian

Submitted Date: 08/21/2026

Inherence comments on how the proposed customer identification program can preserve strong customer-identification requirements while reducing unnecessary compliance burden. We recommend retaining the rule's primary-market focus, preserving technology-neutral digital identity methods, allowing machine-verifiable records to evidence CIP determinations, and permitting per-determination evidence to support reliance on other regulated institutions. These approaches can reduce duplicate verification, unnecessary transmission of sensitive data, and retrospective reconstruction of compliance decisions without weakening the underlying identification standard or shifting responsibility away from the PPSI. We also encourage the Agencies to preserve risk-based flexibility for redemption workflows and to define the regulatory outcomes and assurance required rather than prescribe specific technologies or processes.

Comment of Inherence, Inc. on the Proposed Rule: Permitted Payment Stablecoin Issuer Customer Identification Program

August 21, 2026

Submitted electronically to the Financial Crimes Enforcement Network (Docket No. FINCEN-2026-0101; RIN 1506-AB74); the Office of the Comptroller of the Currency (Docket ID OCC-2026-0331; RIN 1557-AF53); the Board of Governors of the Federal Reserve System (Docket No. R-1885; RIN 7100-AH18); the Federal Deposit Insurance Corporation (RIN 3064-AG28); and the National Credit Union Administration (Docket No. NCUA-2026-0793; RIN 3133-AG09).

Re: Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37,234 (June 22, 2026)

To 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:

I. INTRODUCTION

Inherence, Inc. ("Inherence") builds infrastructure that allows financial institutions to enforce policies and produce independently verifiable evidence that those policies were followed.

We submit this comment principally in response to Questions 1 and 4 through 8. The central recommendation of this comment is simple:

Preserve the required customer-identification outcome, obtain the strongest available evidence that the outcome was achieved, and require no more process, disclosure, or duplication than that outcome demands.

That principle is consistent with the structure of the proposed rule. The Bank Secrecy Act directs the government to establish minimum standards for customer identification. The proposal requires a PPSI to maintain procedures that allow it to form a reasonable belief that it knows the true identity of each customer, while preserving flexibility in the technology used to reach that result. The Agencies likewise declined to impose CIP collection obligations across the secondary market where the issuer ordinarily has no direct customer relationship.

New verification technology creates an opportunity to extend that same approach to the evidence of compliance. A regulated institution increasingly can make a required determination, enforce the resulting decision, and produce evidence of that determination that another authorized institution or examiner can verify independently. Where that is possible, assurance need not depend entirely on repeated collection of the same supporting information, institution-specific reconstruction of prior decisions, or additional prescribed processes. We refer below to such records as machine-verifiable evidence.

This comment does not propose reducing the information a PPSI is legally required to obtain, weakening the standard for verifying customer identity, transferring responsibility away from the PPSI, or replacing records the proposed rule requires. Instead, we recommend that the final rule remain open to technical architectures that can provide the required assurance with less surrounding regulatory machinery.

Inherence has implemented one example. Once the inputs required for a policy decision are available, our system evaluates the action against the applicable policy and produces a compact cryptographic receipt of the determination. In our current measured benchmarks on commodity hardware, producing that receipt takes `2.57 milliseconds`, verification takes `0.96 milliseconds`, and the receipt is `128 bytes`. These figures measure policy evaluation and evidence generation, not the time required for an external identity provider, government database, credential issuer, or other source to produce the underlying information. We provide these figures only to establish feasibility: per-determination compliance evidence can be produced and verified at transaction-system speeds.

EXECUTIVE SUMMARY

Applied to the proposal, the central principle yields five recommendations:

1. **Retain the primary-market perimeter (Question 1).** The issuer's direct relationship, and only that relationship, should give rise to the CIP obligation. Improving verification technology should strengthen assurance where the obligation already exists; it should never become a reason to expand collection.

2. **Preserve technology-neutral identity verification (Questions 5 and 6).** If the final rule addresses digital credentials expressly, it should define their required properties rather than approve particular technologies, and it should let a reliable credential establish a required fact with less duplication of underlying supporting data.

3. **Permit per-determination evidence to support reliance (Question 7).** An annual certification establishes that a program exists. A signed, independently verifiable record establishes that the required procedure was performed for this customer with this result. The rule should allow reliance, including affiliate and third-party service arrangements, to rest on the second, and should write its evidence provisions functionally so that determinations of authority over an account can be evidenced the same way as determinations of identity.

4. **Recognize machine-verifiable records for the "methods and results" component of the CIP record.** A record that binds the governing procedure, its inputs, the time, and the result is stronger evidence than a database field, and recognizing it adds no new compliance obligation.

5 **Preserve risk-based flexibility for redemption-only relationships (Question 4).** However the Agencies resolve when a redemption creates an account, some set of conditions will govern the moment value is released. The rule should require that those conditions actually execute at that moment, enforced automatically in the transaction workflow, with no categorical waiting period or manual process.

II. RETAIN THE PROPOSED PRIMARY-MARKET BOUNDARY

RECOMMENDATION 1

Retain the proposed limitation of CIP obligations to direct relationships with the PPSI.

Question 1 asks whether the proposed CIP requirement should be extended to secondary-market activity. It should not.

The proposal distinguishes the primary market, where the PPSI directly interacts with the user or holder, from secondary-market activity that does not directly involve the PPSI other than through a smart contract. The Agencies recognize that the overwhelming share of stablecoin transaction activity occurs in the secondary market, and that issuers have limited practical ability to obtain customer information there; extending a collection obligation across that activity would, in the Agencies' own assessment, be nearly impossible for PPSIs to implement.[1] For that reason, the proposal confines CIP customer-information collection to primary-market relationships. That is the right regulatory design.

The relevant question should be whether the issuer has the relationship that gives rise to the customer-identification obligation, not whether technology could theoretically make additional information collection possible. Better verification technology should not become a reason to expand the regulatory perimeter. Instead, it should allow the government to obtain stronger assurance where the obligation already exists.

This distinction will become more important as digital identity and verifiable credentials improve. Technology may make it possible for a person to demonstrate particular facts or statuses to another market participant without requiring every intermediary or issuer to establish a new customer relationship. The availability of stronger evidence should therefore support a more targeted regulatory architecture, not justify broader collection by default.

III. PRESERVE TECHNOLOGY-NEUTRAL IDENTITY VERIFICATION

RECOMMENDATION 2

Preserve the proposal's technology-neutral approach to identity verification and, if the final rule addresses digital credentials expressly, define their required properties rather than prescribing particular technologies.

Questions 5 and 6 ask whether the regulatory text should address digital identity solutions

and verifiable credentials. The proposal already identifies the right principle.

FinCEN and the Agencies state that technological variation and innovation are best accommodated by maintaining flexibility in how a PPSI verifies customer identity. They specifically recognize that a nongovernmental digital credential may allow a person to prove who they are without revealing information beyond the fact being established and may, where appropriate under a risk-based procedure, qualify as a non-documentary verification method.[2] We agree.

The rule should specify the assurance the PPSI needs, rather than maintaining an approved list of technical mechanisms. Where a PPSI relies on a digital credential, the relevant questions include whether the responsible issuer can be identified, whether the credential can be authenticated and bound to the customer, whether its scope and assurance level are clear, whether current validity or revocation status can be determined, and whether the PPSI can preserve evidence that it relied upon the credential. This approach allows technology to improve without changing the regulatory outcome.

It also creates an important data-minimization benefit. The proposed rule still requires PPSIs to obtain and retain specified identifying information. Nothing in this comment would alter that obligation. But verifying those facts does not necessarily require every institution to obtain a new copy of every supporting document or dataset another trusted party used to establish them.

A reliable credential can, where appropriate, allow a PPSI to verify the required fact while collecting less additional supporting information. The objective should be: the information required to identify the customer, plus the evidence necessary to establish that the required verification occurred, and nothing additional merely because existing processes make it convenient to copy it. That can reduce operational burden and reduce the number of unnecessary repositories of sensitive customer information without lowering the identification standard.

IV. MAKE RELIANCE WORK AT THE LEVEL OF THE ACTUAL DETERMINATION

RECOMMENDATION 3

Permit per-determination verifiable evidence to support reasonable reliance on another regulated financial institution's CIP.

Question 7 asks how likely PPSIs are to rely on another PPSI's CIP or on the CIP of another federally regulated financial institution.

The proposed rule permits such reliance under specified conditions. Among other things, the relied-upon institution must be appropriately regulated, the reliance must be reasonable, and the institutions must have a contract requiring an annual certification concerning the

AML/CFT program and performance of the specified CIP procedures.[3] Importantly, the proposal preserves the PPSI's responsibility for its own compliance.

The annual certification provides useful program-level assurance: does the institution maintain the required program and agree to perform the specified procedures? But reliance ultimately occurs at another level: was the required procedure actually performed for this customer, and what was the result? The final rule should allow the second question to be answered directly.

A relied-upon institution could produce a signed or otherwise independently verifiable record identifying the institution responsible for the determination, the customer or credential to which it applies, the procedure performed, the result, the time of the determination, and where appropriate its expiration or current validity. The PPSI could retain or reference that determination as part of its CIP records.

This would not eliminate the annual certification. It would not alter the conditions under which reliance is reasonable. And it would not transfer responsibility away from the PPSI where the proposed rule leaves responsibility with the PPSI. It would simply provide more precise evidence for the particular determination on which the PPSI relied. That precision matters most where reliance will be heaviest: in corporate families where a PPSI relies on the program of an affiliated regulated institution, per-determination records let the PPSI and its examiners establish which entity performed which procedure for which customer.

The same record architecture serves a second arrangement the proposal expressly permits: the use of third-party service providers to perform CIP services on the PPSI's behalf, with the obligation remaining on the PPSI.[4] Per-determination records let the PPSI verify what its provider actually did for each customer, rather than relying on the provider's aggregate assurances.

This architecture has already been demonstrated in official-sector research. In Project Mandala, the BIS Innovation Hub and participating central banks developed a system in which financial institutions perform specified compliance checks and produce cryptographic proofs that can accompany a payment instruction (BIS Innovation Hub, *Project Mandala: Streamlining Cross-Border Transaction Compliance*, October 2024). The proof can be verified without revealing the underlying customer data. BIS describes the project as preserving the existing regulatory framework and the responsibility of financial institutions to interpret and apply applicable regulatory measures; the innovation is in how the compliance determination is executed and evidenced.

Mandala is an experimental proof of concept, not an adopted regulatory framework, and it is not a CIP system. Its relevance here is narrower and more important: it demonstrates that a compliance determination can become a portable verification object rather than merely an

assertion inside the institution that originally performed the check. BIS has described this architecture as a way to automate compliance without compromising the quality and soundness of regulatory checks.

The same concept can make CIP reliance more useful. Instead of repeatedly recreating a determination from underlying records, a PPSI can verify evidence of the determination another regulated institution was responsible for making, subject to whatever reliance conditions the Agencies retain. The rule should permit that model.

One further determination will grow in importance over the life of this rule. The proposal already requires, for certain customers, information about individuals with authority or control over an account.[5] As payment stablecoins become programmable at scale, authority over an account will increasingly be exercised by automated systems acting under delegation from an identified principal. Identifying the customer and verifying the authority of the actor operating for that customer are distinct determinations, and the same per-determination evidence serves both: a verifiable record can establish that a specific actor, human or automated, held current, scoped authorization from an identified principal when the action occurred. The Agencies need not resolve questions about automated agents in this rulemaking. It is enough that the evidence provisions be written functionally, so that determinations of authority can be evidenced the same way as determinations of identity.

V. RECOGNIZE STRONGER EVIDENCE WITHOUT REQUIRING IT

RECOMMENDATION 4

Clarify that machine-verifiable records may satisfy the "methods and results" component of the CIP record where they contain the information necessary to demonstrate the relevant determination.

Proposed § 1033.220(a)(3) requires PPSIs to maintain specified records, including customer identifying information, information concerning documents relied upon, and a description of the methods and results of measures undertaken to verify a customer's identity.[6] We do not recommend replacing those required records. We recommend that the final rule remain open to stronger forms of evidence for the methods and results of an automated determination.

Consider the difference. A conventional record may say:

```
KYC_STATUS = PASSED
```

That establishes what the institution's database currently reports. A machine-verifiable record can establish a more specific proposition: that a particular version of a specified procedure, applied to the inputs bound to the record, produced the stated result at a particular time.

Where the relevant inputs come from authenticated sources or credentials, the record can also preserve their provenance.

Such evidence does not establish that an inaccurate underlying source was true. It establishes what procedure was performed, over which bound inputs, when it occurred, and what result it produced. That can give an institution and its examiners more direct evidence of whether the operated program corresponds to the written program.

The Agencies need not mandate cryptographic proofs, particular proving systems, blockchains, or credential protocols. They need only avoid defining the acceptable record in a way that assumes retrospective institutional records are the strongest evidence available. A technology-neutral standard might look instead to functional properties such as contemporaneity, integrity, binding to the applicable procedure and determination, attributable responsibility, independent verification, and appropriate minimization of unnecessary disclosure. That approach adds no new compliance obligation. It simply allows a PPSI to satisfy an existing evidentiary obligation more effectively.

VI. DO NOT TURN THE REDEMPTION TIMING QUESTION INTO AN UNNECESSARY PROCESS REQUIREMENT

RECOMMENDATION 5

For redemption-only relationships, preserve risk-based flexibility and permit automated enforcement of interim-use conditions rather than imposing a categorical new waiting period or manual process.

Question 4 asks whether the proposal should be refined for a customer whose only desired relationship with the PPSI is to redeem a payment stablecoin. The proposal recognizes that a person may obtain a stablecoin elsewhere and approach the PPSI directly for redemption, and that the redemption may itself establish the account relationship.[7] That creates a genuine sequencing issue.

The proposed rule requires identifying information before account opening, while identity verification may occur within a reasonable time after account opening.[8] The CIP must also specify the terms under which a customer may use an account while verification remains incomplete.[9] Because verification may follow account opening, and the redemption may itself open the account, verification may still be pending at the moment value moves. The interim-use terms are the operative protection in exactly that case, and they protect only if they execute.

Commenters will reasonably disagree about when a redemption-only contact creates an account. However the Agencies resolve that definitional question, some set of conditions will govern the moment value is released: completed onboarding, permitted interim activity, or

refusal. Recommendation 5 concerns only that whichever conditions apply actually execute at that moment.

The final rule should not resolve this issue by assuming that every redemption requires an additional manual hold or prescribed waiting period. Instead, it should preserve the existing risk-based framework and allow PPSIs to enforce whatever interim conditions their compliant CIP requires directly in the transaction workflow.

If verification is complete, the transaction can proceed under the institution's policy. If verification remains incomplete but specified activity is permitted, the applicable conditions can be enforced before the relevant action proceeds. If the institution cannot form the required reasonable belief or its policy requires the transaction to stop, the action can be blocked.

The functional pattern is consistent: evaluate before execution, produce independently verifiable records. Enforcement of this kind adds no material delay; in our implementation, the policy evaluation itself completes in tens to hundreds of nanoseconds, so automated enforcement preserves the speed of redemption while the applicable condition governs the transaction. The regulatory objective is that the applicable condition actually governs the transaction, not that every PPSI use the same operational mechanism to achieve that result.

The Agencies' own analysis shows where this matters most. The regulatory impact analysis estimates roughly 50 PPSIs, with an average of approximately 1,000 primary-market customers per issuer, alongside outlier issuers exceeding 250,000 primary-market customers in a single year as wider-facing mint and redeem models spread.[10] At the average scale, manual workflows can survive. At the outlier scale, automated enforcement is the architecture that scales.

This is an important distinction for programmable financial systems. The rule can require the outcome while leaving implementation to the market. Where the final rule additionally permits tiered or simplified treatment of lower-risk redemptions, a per-decision verifiable record of each tiering determination supplies the documentation that makes that flexibility supervisable.

VII. QUESTION 8: INNOVATION CAN REDUCE REGULATORY BURDEN WITHOUT REDUCING REGULATORY ASSURANCE

Question 8 asks what changes would make the proposed rule more conducive to industry innovation and how those changes would affect PPSI operations and illicit-finance risk. Our answer is that the Agencies should apply a consistent principle throughout the final rule:

Specify the required regulatory outcome and the evidence necessary to demonstrate it. Prescribe no additional process or information merely because older technology required it as a proxy for assurance.

This is not an argument for weaker customer identification. It is an argument for distinguishing the regulatory objective from the historically available means of demonstrating it.

A regulator needs confidence that the PPSI obtained the required identifying information, applied an appropriate verification procedure, formed the required reasonable belief about the customer's identity, and complied with the other obligations of its CIP. Traditionally, confidence in those outcomes has depended heavily on process: institutional records, manual review, duplicated documentation, periodic certifications, and retrospective examination. Those mechanisms remain appropriate where needed. But they should not be required solely because they were historically the only practical way to obtain assurance.

Project Mandala illustrates the broader possibility. BIS and participating central banks demonstrated that existing regulatory requirements can remain intact while compliance checks become programmable and their results become independently verifiable. The project expressly preserves the existing regulatory framework; the technical innovation is intended to increase speed and efficiency without compromising the quality of the regulatory checks.

The same design principle can apply here:

same identification standard;
less unnecessary duplication;
less unnecessary disclosure;
stronger evidence of the determination.

This need not increase illicit-finance risk. None of our recommendations reduces the minimum identifying information the proposed rule requires. None changes the standard that the PPSI form a reasonable belief that it knows the true identity of its customer. None eliminates required recordkeeping. None transfers responsibility from the PPSI to an unregulated third party.

Instead, the recommendations can strengthen assurance in four ways. They can make relevant conditions enforceable at the time an action occurs. They can bind a verification result to the procedure and inputs that produced it. They can make reliance on another regulated institution more precise. And they can reduce unnecessary copies of sensitive supporting information while preserving the information the rule actually requires.

There are limits. A cryptographic record cannot make false underlying information true. It cannot determine whether an unreliable credential issuer should be trusted. It cannot substitute for judgment where the governing standard requires judgment. Those questions remain with the responsible institution and the applicable regulatory framework.

Machine-verifiable evidence addresses a narrower problem: once the responsible party has made the required determination, how much additional machinery should be necessary to establish that it actually made it? Increasingly, the answer can be: very little.

VIII. CONCLUSION

The Agencies do not need to choose between innovation and effective customer identification. They can preserve the substantive CIP obligation while allowing institutions to satisfy and evidence that obligation more efficiently.

The proposed rule already takes important steps in that direction. It preserves flexibility in verification methods. It contemplates digital credentials. It permits reliance on other regulated financial institutions. It limits CIP collection to relationships in which the issuer actually has a customer. The final rule should carry that principle through to compliance evidence itself.

Where the Agencies need a regulatory fact, they should define the fact that must be established and the level of assurance required. Where market participants can produce reliable, independently verifiable evidence of that fact with less duplication, less disclosure, and less process, the rule should permit them to do so. The goal is not less assurance. It is the minimum machinery necessary to produce sufficient assurance.

We therefore recommend that the Agencies retain the primary-market CIP perimeter, preserve technology-neutral identity verification, recognize per-determination evidence as a tool for reliance, permit machine-verifiable records to evidence the methods and results of CIP determinations, and preserve risk-based flexibility for redemption workflows.

Inherence would welcome the opportunity to demonstrate these capabilities to the Agencies.

Respectfully submitted,

Jing Jian
Founder and Chief Executive Officer
Inherence, Inc.
Los Angeles, California

inherence.dev

FOOTNOTES

1. Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37,234, 37,239 (June 22, 2026). The Agencies explain that extending CIP to activity in which the user's only interaction with the PPSI is through a smart contract could effectively create a global identity-collection obligation that would be nearly impossible for PPSIs to implement and could potentially cripple the industry.

2. Id. at 37,242. The proposal expressly discusses a nongovernmental digital credential that allows a person to prove identity without revealing information other than that fact, while retaining a risk-based and technology-neutral approach, and requests comment on whether regulatory text should address digital identity.

3. Id. at 37,243-44. Proposed § 1033.220(a)(6) requires, among other conditions, a contract under which the relied-upon institution annually certifies that it has implemented the applicable AML/CFT program and will perform the specified CIP requirements.

4. Id. at 37,243. The proposal states that the reliance provision should not be construed as restricting appropriate use of third parties to perform a service related to a PPSI's CIP on the PPSI's behalf, with the CIP obligation remaining with the PPSI.

5. Id. at 37,242. Proposed § 1033.220(a)(2)(ii)(C) requires a PPSI's CIP to address obtaining information about individuals with authority or control over certain accounts where the customer is not an individual and cannot otherwise be verified.

6. Id. at 37,243. Proposed § 1033.220(a)(3) separately requires identifying information, descriptions of documents, methods and results of verification, and resolution of substantive discrepancies.

7. Id. at 37,239-40. The Agencies specifically identify the case in which a person acquires a stablecoin elsewhere and then approaches the PPSI for direct redemption, which may establish an account and make the person a customer, and request comment on whether the proposal should be refined or clarified to account for such activity.

8. Id. at 37,242-43. The proposal requires a PPSI to obtain identifying information prior to opening an account (proposed § 1033.220(a)(2)(i)) and to verify the identity of each new customer within a reasonable period of time after the account is opened (proposed § 1033.220(a)(2)(ii)); comparison against designated government lists must occur within a reasonable period after account opening unless another applicable authority requires earlier action (proposed § 1033.220(a)(4)).

9. Id. at 37,242-43. Proposed § 1033.220(a)(2)(iii) requires the CIP to address, among other things, the terms under which a customer may use an account while the PPSI attempts to verify identity.

10. Id. at 37,246-48 (regulatory impact analysis). The Agencies estimate approximately 50 PPSIs, an average of approximately 1,000 primary-market customers per issuer, and outlier issuers with more than 250,000 primary-market customers in a given year, and observe that some issuers have increasingly adopted wider-facing mint and redeem models that seek to include smaller investors and businesses.