NETKI, INC., JUSTIN NEWTON

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C22

Subject

Docket No. R-1885; RIN 7100-AH18 — Comment of Netki, Inc.

Submitter Information

Organization Name: Netki, Inc.

Organization Type: Company

Name: Justin Newton

Submitted Date: 08/21/2026

Please see attached PDF letter for comments.

--

[https://signaturehound.com/api/v1/file/de2uokzixspxc]<https://www.netki.com/>

Justin Newton

CEO & Founder

[https://signaturehound.com/api/v1/png/email/default/532e8a.png]

justin@netki.com<mailto:justin@netki.com>

[https://signaturehound.com/api/v1/png/mobile/default/532e8a.png]

(818) 927-2646<tel:8189272646>

[https://signaturehound.com/api/v1/png/map/default/532e8a.png]

Los Angeles, California

[https://signaturehound.com/api/v1/png/website/default/532e8a.png]

netki.com<https://www.netki.com/>

[https://signaturehound.com/api/v1/png/twitter/round/532e8a.png]<https://twitter.com/justinwnewton>

[https://signaturehound.com/api/v1/png/linkedin/round/532e8a.png]<http://linkedin.com/in/justinnewton>

Digital Identity and Compliance Infrastructure

netki.com · justin@netki.com

August 21, 2026

Regulatory and Strategic Affairs Division
Financial Crimes Enforcement Network
P.O. Box 39, Vienna, VA 22183

Chief Counsel's Office, Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 1E-216, Washington, DC 20219

Benjamin W. McDonough, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Washington, DC 20551

Jennifer M. Jones, Deputy Executive Secretary
Attention: Comments—RIN 3064-AG28
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429

Melane Conyers-Ausbrooks, Secretary of the Board
National Credit Union Administration
1775 Duke Street, Alexandria, Virginia 22314-3428

Re: Permitted Payment Stablecoin Issuer Customer Identification Program

> Notice of proposed rulemaking, 91 Fed. Reg. 37234 (June 22, 2026), FR Doc. 2026-12460
>
> FinCEN: RIN 1506-AB74, Docket FINCEN-2026-0101 · OCC: RIN 1557-AF53, Docket OCC-2026-0331
>
> Board of Governors: RIN 7100-AH18, Docket No. R-1885 · FDIC: RIN 3064-AG28
>
> NCUA: RIN 3133-AG09, Docket NCUA-2026-0793

Ladies and Gentlemen:

I. Who Netki is, and why we are commenting

Netki, Inc. builds and operates identity verification and transaction-level compliance systems for regulated financial institutions, including authentication of government-issued

identity documents, biometric binding of a credential to the person presenting it, onboarding of individuals and of legal entities and their control persons, and compliance logic that evaluates digital asset transactions as they occur, among them our Sentinel product for stablecoin issuers. Our verification systems run in production for regulated institutions across multiple jurisdictions, including digital asset identity infrastructure deployed at national scale.

Netki is not a payment stablecoin issuer and does not intend to become one. We are a technology provider to financial institutions that carry the obligations this rule creates, and our commercial interest is plain: if the agencies recognize credential-based verification, preserve room for specialist providers, and expect transaction-level controls, companies like ours benefit. We state that here, and add a specific disclosure in Section VII where the interest is sharpest. Two of our recommendations, in Sections VI.B and VII, would make the rule stricter than proposed.

We have reviewed the comments on Docket FINCEN-2026-0101 and the Board's docket. Several urge the agencies to name verifiable credentials in the regulatory text; one urges the opposite. Where we agree with a position already in the record we say so and explain why; where we depart from both, we set out the alternative.

II. Summary of Netki recommendations

1. **Adopt a performance standard for digital identity credentials used in customer verification.** Implement regulatory text or supervisory guidance describing what a credential must do to support the reasonable belief § 1033.220(a)(2) requires, naming no technology, format, or vendor. (Questions 5 and 6; text at Appendix A, item 1.)

2. **State plainly that verification against a conforming credential satisfies § 1033.220(a)(2)(ii).** We propose, for example, treating a state-issued mobile identification as a documentary method and a conforming non-governmental credential as a non-documentary method, and conforming the recordkeeping provision at § 1033.220(a)(3)(i) so that a credential-based verification produces a complete record. (Questions 5 and 6; Appendix A, items 1–2.)

3. **Open the reliance provision to supervised identity providers by extending the GENIUS Act's own state-certification logic.** Amend § 1033.220(a)(6)(ii) so a Permitted Payment Stablecoin Issuer (PPSI) may also rely on a qualified identity service provider supervised under a state regime certified under section 4(c) of the Act. (Question 7; Appendix A, item 3.)

4. **Adopt a safe harbor for verification performed against the standard**, on the model the OCC has already proposed at 12 CFR 19.262(a) for the AML/CFT program rule. (Question 8; Appendix A, item 6.)

5. **Require verification to be complete before the issuer performs an act it cannot undo.** Where a PPSI will mint or release payment stablecoins and retains no ability to freeze or recall them, identity verification must be finished first. (Question 8; Appendix A, item 5.)

6. **Extend risk-based, transaction-level screening to secondary market activity, with identity supplied by conforming credentials rather than account opening.** Sanctions and designated lists name people. While such lists do include wallet addresses, a bad actor can spin up a new wallet instantly and without permission, so address lists necessarily lag reality. Any screening performed without identity validation should not be considered to meet the minimum threshold for effective screening. Moving forward, a credential verified once to the Section IV standard and presented at each transfer will make real-time identity-aware screening feasible without onboarding secondary-market holders or building CIP files on them. (Questions 1 and 4; Section VII.)

7. **Codify the preamble's assurance that a PPSI may use third parties to perform CIP procedures on its behalf.** The assurance at 91 Fed. Reg. 37243 and footnote 82 rests on a 2005 interagency FAQ and is nowhere reflected in the codified text. The CIP obligation would remain unambiguously with the PPSI. (Question 7; Appendix A, item 4.)

8. **Conform the conjunction in § 1033.220(a)(2)(ii)(B)(2).** The codified text joins the five non-documentary trigger circumstances with "and"; the preamble and Table 3 use "or." Read literally, the codified text requires all five conditions at once. (Appendix A, item 7.)

III. The premise: real-time settlement finality requires real-time compliance

A. Compliance lives in the settlement gap, and payment stablecoins have none

In traditional finance, the transaction and its settlement are separated in time, and the compliance function lives in that gap. If you have worked in compliance, you have lived your career in that gap — and the gap is shrinking. A card authorization precedes settlement by a day or more, an ACH entry can still be returned after it posts, and a securities trade settles the day after it executes. That interval is where the work happens: fraud scoring, screening-hit adjudication, holds on suspicious entries, reversals when something turns out to be wrong. Nearly every control in the bank compliance toolkit assumes that between initiation and finality, the institution has time to look and a mechanism to undo.

A payment stablecoin transfer is not an instruction that settles later. It is the settlement. Transaction and settlement collapse into one atomic, final event, and a control that runs after it prevents nothing. It can record what happened — but by the time a review finds the bad action, the counterparty already has the value.

This is not an argument that digital assets are sui generis. The agencies have met this problem on rails they already supervise: Fedwire transfers are final and irrevocable when made, and RTP and FedNow payments are instant and final. None of those systems answered instant finality by reviewing transactions faster after the fact. Screening and authentication moved in front of the release of funds, since nothing positioned behind an irrevocable payment can stop it. American payment supervisors have confronted this before, and that relocation was the answer.

The consequence for the proposed rule is this: if you are issuing a payment stablecoin, you have to know your customer at the time of reliance, transaction time, not simply the time of account opening. What was true when the account opened may not still be true then. The proposal, drawn from the 2003 bank customer identification rule, is built the other way. It treats verification as a step completed once, around the opening of the relationship, rather than as a condition confirmed at each point of reliance.

B. The rule verifies once, and says so

Proposed 31 CFR 1033.220(a)(2)(ii) requires procedures for verifying identity "within a reasonable time before or after the customer's account is opened." References in this letter to § 1033.220 are to part 1033 of title 31 as proposed at 91 Fed. Reg. 37234. The obligation is anchored to a window solely around account opening. The standard it serves is an outcome standard, namely, risk-based procedures sufficient to "form a reasonable belief that it knows the true identity of each customer," and a belief is a present-tense state. The rule tells an issuer how to form the belief. The rule does not address the consequences when the facts underlying that belief cease to be true, notwithstanding that the issuer will continue to rely on the belief in every subsequent transaction with the customer.

C. The savings clause concedes the transaction, and points at a rule that can no longer be commented on

Proposed § 1033.220(c) provides that nothing in the section relieves a PPSI of its obligation to comply with any other provision of chapter X, "including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction, or its obligations with respect to complying with the terms of any lawful order as set forth in this chapter." The agencies describe the same provision as preserving "requirements to have the technological capability to comply with and to comply with the terms of any lawful order," citing 12 U.S.C. 5903(a)(6)(B) (91 Fed. Reg. 37244 & n.84). The savings clause therefore places both "transaction" and the lawful-order obligation inside the CIP rule's own text.

The obligation it points at is continuing. The companion FinCEN/OFAC program rule proposes, at § 1033.210(b)(1)(iii), that a PPSI "[c]onduct ongoing customer due diligence, including to … [c]onduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information" (91 Fed. Reg. 18582, April 10, 2026). That is the same "maintain and update" duty carried forward from the bank CDD rule, and it is open-ended.

So the identity lifecycle is split across two rulemakings: this one owns formation of the belief and stops at account opening; the program rule owns maintaining customer information to be current and does not provide guidance defining how a verification should be refreshed. The comment period on the program rule closed June 9, 2026. This docket is therefore the only remaining forum in which the seam between them can be raised — a sequencing artifact of a tight statutory timeline, but worth stating plainly. Neither rule says how a verification performed under § 1033.220 persists, decays, or is re-established when the facts change, and for an instrument that settles atomically, that silence is precisely where the risk occurs.

Sections IV through VI are our answers to Questions 5, 6, 7 and 8 in light of that premise. Section VII answers Questions 1 and 4, on secondary market activity and the redemption-only customer, and carries a specific disclosure of our commercial interest in that recommendation.

IV. Questions 5 and 6 — a performance standard, not a technology list

A. The agencies' hesitation is correct, and it points at a standard rather than at silence

The agencies decline to propose regulatory text on verifiable credentials because "[t]hese tools vary in how they operate and in their trustworthiness" (91 Fed. Reg. 37242). We agree, and we would go further: naming any standard, format, or technology in the CFR would freeze a moving market, function as a whitelist regardless of intent, and be least current at the compliance date twelve months after the final rule. The agencies' own impact analysis had to clarify that the listed verification methods "are not meant to be an exclusive list" (91 Fed. Reg. 37256) — evidence of how enumerations get read.

But variation in trustworthiness is an argument for describing what a trustworthy credential does, not for saying nothing. A performance standard names no technology and disadvantages no future scheme; it gives issuers a bar to clear, examiners a bar to examine against, and the market a reason to compete on meeting it.

B. The standard: five properties, stated as outcomes

A digital identity credential used in customer verification should be one for which the issuer's procedures address:

1. **Binding.** The credential is bound to the person or entity presenting it, and the binding is demonstrable at the time of presentation rather than assumed from possession. The binding step is where verification is most likely to fail, because a genuine credential presented by someone other than its subject defeats every downstream cryptographic check. A standard that stops at "the signature validated" would be weaker than the current text, not stronger.

2. **Accountable issuance.** The credential's issuer is identifiable, and the basis of issuance is auditable by the relying institution and its examiners.

3. **Current status, checkable at the time of reliance.** The credential carries a status that can be checked when it is relied upon, so that revocation, expiry, or a material change is visible to the relying party at that moment rather than at the next manual review.

4. **Data minimization.** The credential can establish the required fact without transferring more than that fact — the property the agencies themselves describe at 91 Fed. Reg. 37242 ("prove that they are who they claim to be without revealing information other than that fact"). One boundary matters and should be stated: minimization operates downstream of the verifying institution, not between the customer and the institution at onboarding. The PPSI must hold the full identifying

information § 1033.220(a)(2)(i) specifies, because the § 1033.220(a)(4) list determination and independent sanctions obligations cannot be discharged against a predicate proof — the institution must be able to re-run screening when a list changes and act on a later designation. Completeness at the point of verification; minimization in what is disclosed onward and retained in raw form.

5. **Provenance.** The relying institution can produce a record of what was asserted, by whom, as of when, and with what result, sufficient for § 1033.220(a)(3).

C. Property 3 is the one the premise requires

A document-based verification is a photograph of a fact. It cannot report that it has stopped being true. A credential with checkable status can — which makes it the only verification method that connects this rule to the program rule's duty to "maintain and update customer information," and the only one that can be current at the moment of reliance rather than at the moment of onboarding. This is why the settlement-finality premise in Section III and the digital-identity questions in this rulemaking are the same subject. The agencies do not need to mandate re-verification. They need to recognize the one method that makes re-confirmation cheap enough to be routine, and let risk-based procedures decide the intervals.

We note that transaction-time compliance evaluation is not theoretical. Because a payment stablecoin is implemented as a smart contract, compliance logic can be integrated with the token contract itself and evaluate a transfer at the moment it occurs; systems that do this are in production today, ours among them. The question before the agencies is not whether verification can keep pace with atomic settlement — it can — but whether the rule's vocabulary will recognize the methods that do.

D. Two textual defects the standard should cure

The documentary prong is written for artifacts an analyst inspects. The preamble says a state-issued mobile identification "could constitute" documentary evidence under § 1033.220(a)(2)(ii)(A) (91 Fed. Reg. 37242), but the codified text asks the CIP to "set forth the documents the permitted payment stablecoin issuer will use" and illustrates with "a driver's license or passport." A mobile credential presentation is a signed data structure validated against the issuing authority's certificate chain; what makes it trustworthy is the signature and the trust list, not "a photograph or similar safeguard." A compliance officer reading the codified text has no path to it; one reading the preamble has assurance and nothing to cite in an examination.

The recordkeeping provision makes the higher-assurance path produce the weaker record. Section 1033.220(a)(3)(i)(B) requires the record to note "the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date." Under selective disclosure, several of those elements are never transmitted — by design. Meanwhile the elements that actually evidence a credential-based verification — issuer identity, validation result, binding method, status at the time of verification — appear nowhere in § 1033.220(a)(3)(i). An issuer that accepts a state mobile credential creates a facially incomplete record; one that photographs a plastic

card creates a facially complete record whether or not the card was genuine. Record requirements, not verification requirements, determine what compliance functions collect; until this is conformed, preamble encouragement will not move practice. Operative text at Appendix A, items 1 and 2.

Our second recommendation, stated plainly: say in the regulatory text, or in guidance an examiner can be pointed at, that verification against a credential conforming to the standard satisfies § 1033.220(a)(2)(ii) — the documentary prong where the credential conveys a government-issued identification, the non-documentary prong where it conveys a conforming assertion — and conform § 1033.220(a)(3)(i) so the record of that verification is a record of what made it reliable. One further sentence in the preamble matters as much as either: a status determination properly made and recorded at the time of verification is not retroactively impeached by a later revocation or a later change in the issuer's standing. Without that, careful counsel will steer institutions away from the better method, and the flexibility the agencies intend will go unexercised.

E. The risks, honestly stated

Three risks deserve the agencies' attention more than the ones usually listed. **Enrollment and binding failure** — addressed by properties 1 and 2, and the reason biometric comparison of presenter to subject remains necessary rather than optional. **Revocation infrastructure** — a credential whose status cannot be checked is a document with better marketing; property 3 must be load-bearing, not aspirational. **Uneven availability** — as government and commercially issued credentials are still growing in availability and adoption, credential coverage varies by state, age, immigration status, and device access, and non-U.S. persons sit largely outside U.S. schemes; recognition must be permissive and additive. Section 1033.220(a)(2)(ii)(B)(2) already requires non-documentary procedures for the person unable to present standard identification; for some populations that fallback is the main path, and the rule should not create a compliance incentive to prefer credential-holding customers.

V. Question 7 — reliance, and who is allowed to be relied upon

A. As drafted, the reliance provision will go almost unused

Formal reliance under § 1033.220(a)(6) will be rare — rarer than the 14,575-institution population in Table 2 (91 Fed. Reg. 37249) implies, and FinCEN's own instinct that participation is "unlikely" (91 Fed. Reg. 37248) is right. The annual certification at (a)(6)(iii) is the binding constraint: an institution is asked to attest annually, in an examination-relevant and discoverable writing, to its performance of a third party's regulatory program — an undertaking whose downside is asymmetric to whatever the contract provides in return, and which the relied-upon institution must renew every year for as long as the arrangement lasts. The Federal/State asymmetry the agencies acknowledge (91 Fed. Reg. 37243) removes the most natural pairing. And the counterparties a PPSI actually faces in the primary market — exchanges regulated as money services businesses, foreign virtual asset service providers — sit outside (a)(6)(ii) entirely, because none is regulated by a Federal functional regulator. The provision is most available where it is least needed,

between affiliated bank-supervised entities that would operate an enterprise-wide CIP anyway (91 Fed. Reg. 37241).

What will emerge instead is shared verification infrastructure: multiple institutions using the same systems, and increasingly the same reusable credential, while each performs and documents its own CIP. The proposal accommodates that today only through the preamble's assurance that the rule "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" (91 Fed. Reg. 37243, n.82) — an assurance whose sole cited authority is a 2005 interagency FAQ, and which the codified text nowhere reflects. We ask that it be codified, with the CIP obligation remaining unambiguously with the PPSI. Text at Appendix A, item 4.

B. The structural point: reliance already accepts portable assurance — it just restricts who may supply it

Section 1033.220(a)(6) is the one place in this rule where the framework already accepts a verification someone else performed. Portable identity assurance is not an industry novelty being smuggled in; it is in the proposal. The provision simply restricts the channel to institutions "regulated by a Federal functional regulator" — which forecloses a category the GENIUS Act itself went to some lengths to create room for: state supervision.

The Act built a state track. Under section 4(c) (12 U.S.C. 5903(c)), a state qualified payment stablecoin issuer with not more than $10 billion outstanding may operate under a state regime that is "substantially similar" to the federal framework; Treasury has proposed the broad-based principles for that determination (91 Fed. Reg. 16844, April 3, 2026), and certifications are reviewed by the Stablecoin Certification Review Committee. States are moving: the New York Department of Financial Services proposed a framework expressly designed to obtain certification on June 9, 2026, and other states with prudential digital asset regimes are positioned to follow, including under the Act's expedited path for regimes in effect before enactment (GENIUS Act § 4(c)(7)).

Section 4(c) certifies state regimes for *issuers*. Our ask borrows its logic for one adjacent category: a state regime certified as substantially similar should also be able to qualify and supervise **identity service providers** whose CIP performance a PPSI may rely on. The mechanism for judging whether a state's supervision meets the federal bar already exists; extending it to a verification provider is not a new kind of judgment, only a new application of one. The existing conditions at (a)(6)(i) and (iii) — reasonableness, contract, annual certification — carry over, conformed as shown in Appendix A, and the PPSI remains responsible for its own compliance. Should the agencies prefer not to amend (a)(6), a narrower path remains. Section 1033.220(b) permits the appropriate Federal functional regulator, with the concurrence of the Secretary, to exempt any permitted payment stablecoin issuer from the requirements of this section. That authority could be exercised to relieve a PPSI of the Federal-functional-regulator condition in paragraph (a)(6)(ii) where the provider it relies on is qualified and supervised under a certified state regime and meets the standard described in Section IV. We note this is an issuer-by-issuer remedy rather than a rule of general application, and prefer the amendment for that reason.

The honest counterargument: a federal-charter requirement is a bright line, and "qualified under a certified state regime" asks the agencies to trust a certification process still being written. We would answer that the GENIUS Act already requires exactly that trust for issuers themselves — an issuer's entire compliance program can live under a certified state regime — so declining to extend it to the narrower function of identity verification protects nothing the statute has not already opened.

VI. Question 8 — what would actually make the rule more conducive to innovation

A. A safe harbor, on the agencies' own model

The single biggest suppressor of verification innovation is not any provision of this rule; it is that no issuer wants to be the first examined on a novel method with no stated bar to have cleared. Issuers therefore default to the most conservative method available — document-image capture — whatever the preamble encourages.

The agencies have already decided, in this same rulemaking family, that a safe harbor is the answer to that dynamic at the program level. The OCC's companion proposal provides that, except for "a significant or systemic failure," a PPSI that has established an effective AML/CFT program "will not be subject to an AML/CFT enforcement action or to a significant AML/CFT supervisory action" (proposed 12 CFR 19.262(a), 91 Fed. Reg. 37840, June 24, 2026). The same logic applies with more force to customer identification, because the method-level uncertainty is sharper. We ask for its analog here: an issuer that verifies against a conforming credential, and re-confirms status at the intervals its risk-based procedures specify, is deemed to have formed and maintained the reasonable belief § 1033.220(a)(2) requires, absent a significant or systemic failure. The same protection should extend to a verification performed under paragraph (a)(2)(ii)(B) where the customer is unable to present a conforming credential, so that the harbor rewards the quality of the verification rather than the customer's access to a credential scheme. Text at Appendix A, item 6.

B. Verification before the irreversible act — a place the rule should be tighter

Here the premise in Section III meets the text. Section 1033.220(a)(2)(ii)'s "before or after" window, § 1033.220(a)(2)(iii)(B)'s interim-use provision, and (a)(2)(iii)(C)'s account-closure remedy are all settlement-gap provisions. For a bank they are controlled-exposure decisions: the unverified customer's funds remain in the institution's hands, and closing the account is a real remedy. For a PPSI, "use of the account while verification is pending" means minting and releasing a bearer instrument, and once tokens have moved on-chain, closing the account accomplishes nothing — the value is in the secondary market this rule has just excluded. The remedy operates on the relationship; the risk has already left through the instrument. As drafted, the rule authorizes a compliance posture in which the harm completes before the control finishes running.

We therefore ask the agencies to provide that where a PPSI will mint or release payment stablecoins and does not retain the technical capability to freeze, recall, or render them

unusable, verification must be complete before issuance. Where the issuer does retain that capability, issuance before completed verification remains available under risk-based conditions the CIP specifies in advance — including what the issuer will do about outstanding tokens if verification fails. Keep "before" in (a)(2)(ii); narrow "after" for the issuance case; leave it intact for custodial and reserve-management relationships where it belongs. Text at Appendix A, item 5.

Three things this ask does not do. It does not require anyone to build freeze capability — an issuer without it verifies first, which is where instant-payment institutions already stand. For this purpose, capability means the ability to act on the issuer's own initiative against tokens it has issued; the order-triggered capability the statute requires of every issuer is not, by itself, enough (Appendix A, item 5). It does not mandate exercising the capability in any case; it requires having decided. And it does not conflict with the flexibility we defend elsewhere: a performance standard plus a reusable credential is precisely what makes verification-before-issuance fast enough to be commercially tolerable. We recognize a commenter asking for a stricter rule is unusual. We ask because the alternative is a rule that permits an issuer to put an irreversible instrument into circulation for a person it has not identified, and to document afterward that it could not.

Nor is the ask novel. Congress has already legislated its premise: a PPSI "may issue payment stablecoins only if the issuer has the technological capability to comply, and will comply, with the terms of any lawful order" (GENIUS Act § 4(a)(6)(B), 12 U.S.C. 5903(a)(6)(B)), and a lawful order is defined as one requiring the issuer to "seize, freeze, burn, or prevent the transfer" of its stablecoins (§ 2(16), 12 U.S.C. 5901(16)) — issuance is statutorily conditioned on control capability. The law-enforcement constituency has pressed the same principle to Congress: the National Sheriffs' Association, writing to Senate leadership on separate digital asset legislation, warned against changes that would make it harder to "prevent financial crimes before they occur" and would "reduce opportunities to recover stolen assets" (Letter to Senate Leadership on the CLARITY Act, July 31, 2026). And the sequencing principle has been stated in a companion docket even by commenters seeking flexibility: the Blockchain Association, resisting a fixed redemption timeline in its comment on the OCC's PPSI AML/CFT proposal, argued that any such timeline should begin to run only after onboarding, know-your-customer, AML, and sanctions screening are complete (Comment on Docket OCC-2026-0463, July 24, 2026). Verification before value moves is the shared premise of the statute, of the law-enforcement constituency, and of the industry's own redemption position. Our ask is that the CIP rule state it for issuance, where the same logic applies with at least equal force.

C. Two conforming fixes

The conjunction in § 1033.220(a)(2)(ii)(B)(2). The codified text joins the five non-documentary trigger circumstances with "and"; the preamble (91 Fed. Reg. 37242) and Table 3 (91 Fed. Reg. 37252) use "or." Read literally, the text requires all five at once. Replace "and" with "or." (Appendix A, item 7.)

The recordkeeping conformance described in Section IV.D, without which the safe harbor cannot function — an issuer cannot be safe-harbored on a record the rule gives it no way to make complete.

VII. Questions 1 and 4 — extend identity-aware screening to the secondary market, without extending account opening

Question 1 asks whether any CIP requirement should be extended to secondary market activity, and in what circumstances. Our answer is yes — and the circumstances follow from distinguishing the two things every mature payment system keeps separate. The agencies do not dispute the underlying risk: they describe the secondary market as "the location of significant activity, and potentially significant risk," while noting that issuers have "a limited ability to collect customer information" there (91 Fed. Reg. 37259). Our recommendation addresses the second observation without asking issuers to do the thing the agencies rightly find impracticable.

A card payment system separates two functions. Issuing institutions identify their cardholders once, at onboarding, under their own customer identification obligations. Every transaction is then authorized individually at transaction time and screened by the regulated institutions on each side of it, informed by who the parties are and without re-onboarding anyone. The two layers answer different risks: identification answers *who is this*, and transaction control answers *should this transfer happen* — and the second question cannot be answered well without access to the first.

The agencies have drawn this line halfway. The companion AML/CFT proposal requires PPSIs to maintain the technical capabilities, policies, and procedures to block, freeze, and reject impermissible transactions with regard to the secondary market, and to comply with lawful orders — both, as FinCEN notes, obligations "imposed on PPSIs directly by the GENIUS Act" (91 Fed. Reg. 18592). But FinCEN is "not proposing to require a PPSI as part of an AML/CFT program to monitor secondary market activity," and declined to extend suspicious activity reporting to secondary-market transfers; it requested comment on that approach. Our answer is that the agencies have mandated a control and omitted the circumstances in which an issuer is expected to determine that it should be used — for an instrument that is instant, global, high-value, and final at settlement. We ask them to supply the trigger, and nothing more.

The agencies' stated concern about a broader extension is precise, and we share it. A CIP obligation reaching every transfer "would essentially impose on PPSIs a global obligation to collect and verify identifying information of individual users," which the agencies assess "would be nearly impossible for PPSIs to implement and could potentially cripple the industry" (91 Fed. Reg. 37239). We agree, and we do not ask for it. Nothing in this recommendation would make a secondary-market holder a customer, create an account relationship, or require a CIP record. What we propose operates on the other layer entirely: screening at the moment of transfer, informed by an identity established once and presented by credential.

Why screening without identity is not screening. While wallet address sanctions exist, the lists that matter most name people. A sanctions determination, a designated-list comparison, a politically-exposed-person check — each is a question about *who* is transacting, and address-level heuristics answer it only for counterparties already known to be bad. Left as proposed, the rule produces this result: a sanctioned individual who cannot pass the issuer's front door acquires the same instrument in unlimited size on the secondary market, because the only identity control lives at a door he never has to walk through. For an instrument intended to function as money at global scale, an identity regime that applies only to the roughly one percent of activity in the primary market — the agencies put it at "approximately 99 percent" of stablecoin transaction activity occurring on the secondary market (91 Fed. Reg. 37259) — is not a conservative design choice; it is a routing instruction for evasion.

What should extend: risk-based transaction screening, with identity established to the same standard as at onboarding. The screening that runs at a secondary-market transfer should be able to draw on identity of the same quality the rule requires at issuance — established once, through verification meeting the performance standard in Section IV, and presented thereafter as a conforming credential. This is where the two halves of this letter meet. A reusable credential is verified once and presented repeatedly at negligible marginal cost, which is precisely what makes real-time sanctions and politically-exposed-person screening feasible at the moment of transfer without re-onboarding anyone. Identity at the transaction is what makes list screening effective; the credential is what makes it cheap; and the settlement-finality premise of Section III is why it must run before the transfer completes rather than after. The agencies have identified the gap precisely: exchange operators facilitating off-chain activity "collect customer information in a manner similar to the information collected by issuers for their primary market customers. However, exchanges rarely share this information with issuers" (91 Fed. Reg. 37259). Identity exists; it simply does not travel. A credential verified once and presented at the transfer closes that gap without any information-sharing arrangement between competitors, any account relationship, and any CIP record for a secondary-market party.

What should not extend: the account-opening apparatus. A secondary-market holder does not become the issuer's customer, and the issuer should not be required to build § 1033.220(a)(2)(i) collection files on parties it has no relationship with. Where no conforming credential is available, substituting chain-analytic inference or unattested third-party data *into a CIP record* would manufacture false assurance — a record that looks like a verification and is not one — and examiners and courts would later rely on it. The distinction is between identity *asserted and validated at the moment of a transfer decision*, which should extend, and identity *collected into an account record*, which should not. A credential presentation meeting the Section IV standard is real verification — bound, status-checked, attributable to an accountable issuer — which is exactly what separates it from the inference-based substitutes we caution against.

The capability exists, and the statute assumes it. Congress conditioned the right to issue on control over the instrument in circulation: a PPSI "may issue payment stablecoins only if the issuer has the technological capability to comply, and will comply, with the terms of any lawful order" (12 U.S.C. 5903(a)(6)(B)), where a lawful order is one requiring the issuer to

"seize, freeze, burn, or prevent the transfer" of its stablecoins (12 U.S.C. 5901(16)) — a capability that operates almost entirely in the secondary market, and one the CIP rule's own savings clause keeps in view (Section III.C). The agencies themselves observe that issuers use smart contracts to "enable or prohibit subsequent transactions" (91 Fed. Reg. 37237). Because a payment stablecoin is implemented as a smart contract, the same integration that can prohibit a transfer under a lawful order can evaluate a transfer — including a credential presentation — before it completes; systems doing this are in production today. The capability to act on a lawful order is narrower than the capability to screen: an order names its targets with reasonable particularity, while screening must evaluate every transfer. But the integration point is the same, and an issuer that has built one has built the harder half of the other. What is missing is not the hook into the transfer; it is the identity to evaluate against, which is what a conforming credential supplies.

The obligation is not hypothetical, and it is not new. Treasury has stated that a U.S. person stablecoin issuer "would engage in a prohibited provision of services to a blocked person if it allowed the blocked person to engage with the stablecoin issuer's smart contract to facilitate trades of stablecoins on the secondary market," and that the issuer would be "required to block such stablecoins because the blocked person has an interest in the stablecoins, which the issuer controls via its smart contract" (91 Fed. Reg. 18589). Liability is strict: OFAC "may impose civil penalties for sanctions violations on a strict liability basis." *Id.* An issuer therefore already carries secondary-market sanctions exposure that it cannot discharge without knowing who is transacting — and the proposal, as drafted, supplies no expectation, no method, and no safe path for finding out. We are not asking the agencies to create an obligation. We are asking them to describe how an existing one can be met.

Disclosure, because it is owed here specifically: Netki builds and sells transaction-time screening and control infrastructure for stablecoin issuers, and is developing reusable-credential infrastructure of the kind this recommendation contemplates. This recommendation, if adopted, would expand the market for both. We make it anyway, for the reason stated in Section III — a control positioned after an atomic, final transfer documents harm rather than preventing it, and the only screening that can prevent anything on this instrument runs before the transfer completes.

The circumstances, concretely. We recommend the agencies state — in the final rule here, or in the coordinated finalization of the companion AML/CFT rulemaking to which counterparty screening was deferred — that a PPSI's risk-based program is expected to include transaction-level screening of secondary-market transfers of its stablecoins, encompassing sanctions and designated-list screening informed by identity established to the standard of Section IV and presented by conforming credential, calibrated by risk and by the issuer's retained control capability. Three boundaries keep this proportionate. Identity at the transaction is established by credential presentation, not by document collection, and creates no account relationship or CIP record for secondary-market parties. Consistent with the boundary stated in Section IV.B, property 4, the presentation conveys the identity attributes screening actually requires — not a bare yes-or-no proof; what is dispensed with is the account file, not the identity. And because screening runs at each transfer, a designation made after one transfer is caught at the next, without the issuer

retaining anything between them. The expectation is risk-based — thresholds, velocity, and exposure determine intensity, as they do in every screening regime the agencies supervise. And it keys to the issuer's technical reach, so an issuer is answerable for the transfers it can see and affect, not for activity beyond its protocol. We note the agencies' finding that a majority of transaction volume occurs off-chain, with roughly 35 percent estimated to occur on-chain among the four largest products (91 Fed. Reg. 37259 & n.173); the expectation we describe is calibrated to that finding. It reaches the transfers an issuer can see and affect through its own contract, and no further — while for off-chain activity, the same credential presented at the exchange closes the identity gap the agencies describe, without new obligations on the issuer. At minimum, the final rule should not do the opposite: the preamble's limited-ability observation, quoted above, is accurate as to information collection and says nothing about transactional control; if it survives into the final rule unqualified, it hands an issuer's counsel the argument that it could not have complied with the lawful order the statute made a condition of its license.

The drawbacks, and why they are containable. Question 1 also asks for the benefits and drawbacks of any extension, and two costs deserve statement. First, credential coverage is uneven — by state, age, immigration status, and device access — and non-U.S. persons sit largely outside U.S. schemes; the expectation must therefore be risk-based and must never disadvantage the holder who arrives without a conforming credential, for whom the § 1033.220(a)(2)(ii)(B) path remains the main route. Second, where no conforming credential is available, there is a temptation to substitute chain-analytic inference; as discussed above, that substitutes a guess for a verification, and the final rule should expressly discourage it. Against these, the benefit is that the control the agencies have already mandated becomes usable, and the sanctions exposure issuers already carry on the secondary market becomes dischargeable.

Question 4 — the redemption-only relationship. The agencies describe an individual who acquires a payment stablecoin from an exchange and then seeks to redeem it with the issuer, observing that "[t]hat redemption could establish an account with the PPSI and make the individual a customer," and ask whether the rule should be refined to account for that situation (91 Fed. Reg. 37239). This is the clearest case for a conforming credential in the entire rulemaking. The issuer has no prior relationship, no existing file, and no operational reason to open one; the customer has a single transaction in view. Full account-opening collection is disproportionate to that relationship, and identity assurance is nonetheless essential, because redemption is where value leaves the instrument and enters the banking system. We recommend the agencies state that verification through a credential conforming to the standard in Section IV satisfies § 1033.220(a)(2)(ii) for a customer whose only relationship with the issuer is redemption, and that the record described in Appendix A, item 2 is a complete CIP record for such a customer.

VIII. Conclusion

We support this rulemaking, and our asks are few. Describe what a credential must do rather than naming one — the performance standard. Say that verification against a conforming credential satisfies the rule, and let the record of it be complete. Open the reliance channel to identity providers supervised under the state track the GENIUS Act

itself created. Give issuers a safe harbor on the model the OCC has already proposed, so no one has to be first against an unstated bar. Close the gap the borrowed bank architecture leaves open, by requiring verification before the act that cannot be undone. Codify the third-party assurance the preamble already gives, and correct the conjunction that makes five trigger circumstances read as one. And match the control to the instrument: verify identity once, to a standard worth reusing — then let every transfer, on either side of the primary-market line, be screened in light of it.

The thread through them all is the one stated at the outset: payment stablecoins settle atomically, so compliance must be current at the moment it is relied upon. The agencies' proposal already contains every raw material needed — an outcome standard, a risk-based frame, a reliance mechanism, a savings clause pointing at the continuing duty, a statutory control capability, and a state track. Our recommendations connect them.

We would welcome the opportunity to discuss any of this with the agencies' staff. Thank you for your consideration.

Respectfully submitted,

Justin W. Newton
Founder and Chief Executive Officer
Netki, Inc.
justin@netki.com

Appendix A — Proposed regulatory text

Drafted to name no standard, format, technology, or provider. A credential scheme that does not yet exist would qualify on the same terms as one that does.

1. Add § 1033.220(a)(2)(ii)(D) — verification through conforming digital identity credentials

(D) Verification through digital identity credentials. A permitted payment stablecoin issuer may verify the identity of a customer, in whole or in part, by validating an electronically transmitted credential or assertion concerning the customer. For a permitted payment stablecoin issuer relying on such a credential, the CIP must contain procedures that provide for:

(1) Determining that the credential is bound to the customer presenting it, by means demonstrable at the time of presentation;

(2) Identifying the credential issuer and determining that reliance on credentials issued by that issuer is reasonable under the circumstances;

(3) Validating the authenticity and integrity of the credential by cryptographic or other reliable means;

(4) Determining the status of the credential at the time of verification and, where the permitted payment stablecoin issuer's risk-based procedures so provide, at subsequent times of reliance; and

(5) Making and retaining the records described in paragraph (a)(3)(i)(C) of this section.

Where such a credential conveys the content of an identification document described in paragraph (a)(2)(ii)(A) of this section, the permitted payment stablecoin issuer may treat the verification as verification through documents; where it conveys an assertion concerning the customer without conveying such content, the permitted payment stablecoin issuer may treat the verification as a non-documentary method under paragraph (a)(2)(ii)(B) of this section. Verification performed in accordance with this paragraph (a)(2)(ii)(D) satisfies the requirement of paragraph (a)(2)(ii) of this section, provided the permitted payment stablecoin issuer has performed and recorded the procedures described in paragraphs (D)(1) through (5). Nothing in this paragraph (a)(2)(ii)(D) relieves a permitted payment stablecoin issuer of the requirement to obtain the information specified in paragraph (a)(2)(i) of this section.

Conforming change to the (a)(2)(ii) chapeau: revise the final sentence to read, "The procedures must describe when the permitted payment stablecoin issuer will use documents, non-documentary methods, a method described in paragraph (a)(2)(ii)(D) of this section, or a combination of such methods, as described in this paragraph (a)(2)(ii)."

The satisfaction sentence is deliberate: the preamble already says a conforming credential "could" serve (91 Fed. Reg. 37242), and permission a compliance officer cannot cite in an examination changes no behavior. The final sentence forecloses the reading that a PPSI may onboard a customer it cannot name, which would collide with § 1033.220(a)(4) and independent sanctions obligations (Section IV.B, property 4).

2. Amend § 1033.220(a)(3)(i)(B) and (C) — records of credential-based verification

Add at the end of (B):

Where the content of such a document was conveyed by means of a credential under paragraph (a)(2)(ii)(D) of this section rather than relied on under paragraph (a)(2)(ii)(A), the record must include such of these elements as were conveyed, together with the information described in paragraph (a)(3)(i)(C) of this section.

Revise (C) to read:

(C) A description of the methods and results of any measures undertaken to verify the identity of a customer under paragraphs (a)(2)(ii)(B), (C), and (D) of this section and, for a verification under paragraph (a)(2)(ii)(D), the identity of the credential issuer, the means by which the authenticity and integrity of the credential were validated and the result, the means by which the credential was determined to pertain to the customer, and the status of the credential as determined at the time of verification;

We further request preamble text confirming that a status determination properly made and recorded at the time of verification is not impeached by a later revocation of the credential or change in the standing of its issuer.

3. Amend § 1033.220(a)(6) — reliance on supervised identity service providers

Revise the (a)(6) chapeau to read:

(6) Reliance on another financial institution or other person. The CIP may include procedures specifying when the permitted payment stablecoin issuer will rely on the performance by another financial institution (including an affiliate), or by another person described in paragraph (a)(6)(ii)(B) of this section, of any procedures of the permitted payment stablecoin issuer's CIP, with respect to any customer of the permitted payment stablecoin issuer that is opening, or has opened, an account or has established an account or similar business relationship with that financial institution or other person to provide or engage in services, dealings, or other financial transactions, provided that:

Revise (ii) to read:

(ii) Either—

(A) The other financial institution is subject to a rule implementing 31 U.S.C. 5318(h) or 12 U.S.C. 5903(a)(5)(A) and is regulated by a Federal functional regulator; or

(B) The other person is a qualified identity service provider subject to supervision and examination under a State-level regulatory regime that has been certified under section 4(c) of the GENIUS Act (12 U.S.C. 5903(c)) and that includes standards for the licensing, supervision, and examination of identity service providers; and

Revise (iii) to read:

(iii) The other financial institution or other person enters into a contract with the permitted payment stablecoin issuer requiring it to certify annually to the permitted payment stablecoin issuer that it has implemented its AML/CFT program or, in the case of a person described in paragraph (a)(6)(ii)(B) of this section, that it remains in good standing under the certified State-level regulatory regime under which it is supervised, and that it will perform (or its agent will perform) specified requirements of the permitted payment stablecoin issuer's CIP.

Condition (i) applies unchanged. In the alternative, § 1033.220(b) would permit the appropriate Federal functional regulator, with the concurrence of the Secretary, to exempt a permitted payment stablecoin issuer from the Federal-functional-regulator condition on an issuer-by-issuer basis; we prefer the amendment as a rule of general application.

4. Add § 1033.220(a)(7) — use of service providers

(7) Use of service providers. A permitted payment stablecoin issuer may enter into an arrangement with any person to perform, on the permitted payment stablecoin issuer's behalf, any procedure of the permitted payment stablecoin issuer's CIP. Such

an arrangement is not reliance within the meaning of paragraph (a)(6) of this section, and the person performing the procedure need not be a financial institution or be regulated by a Federal functional regulator. The CIP must address the selection and oversight of any person performing a procedure under this paragraph (a)(7). The CIP obligation, and responsibility for compliance with this section, remain with the permitted payment stablecoin issuer.

This codifies the preamble statement at 91 Fed. Reg. 37243 and footnote 82, whose only current authority is a 2005 interagency FAQ.

5. Add § 1033.220(a)(2)(iv) — timing of verification relative to issuance

(iv) Timing of verification relative to issuance. Where an account involves the issuance, minting, or release of payment stablecoins to or at the direction of a customer, the CIP must specify the point at which verification under paragraph (a)(2)(ii) of this section must be completed. Verification must be completed before the permitted payment stablecoin issuer issues, mints, or releases payment stablecoins to or at the direction of the customer, unless the permitted payment stablecoin issuer retains, and its procedures provide for the exercise of, the technical capability to freeze, recall, or otherwise render unusable the payment stablecoins so issued. Where the permitted payment stablecoin issuer relies on that capability, its procedures must: (1) establish the conditions and limits under which issuance before completed verification is permitted; (2) provide for determining, before issuance, that the capability is effective with respect to the payment stablecoins to be issued; and (3) specify the actions the permitted payment stablecoin issuer will take with respect to payment stablecoins already issued if verification is not completed, including the circumstances in which the capability will be exercised.

Add at the end of the proposed paragraph (a)(2)(iv):

> For purposes of this paragraph (a)(2)(iv), the technical capability to freeze, recall, or otherwise render unusable payment stablecoins means capability exercisable by the permitted payment stablecoin issuer on its own initiative and without a lawful order, with respect to payment stablecoins it has issued to a customer whose verification has not been completed. This capability is distinct from, and not satisfied solely by, the technological capability to comply with a lawful order required by 12 U.S.C. 5903(a)(6)(B).

Conforming additions: at the end of (a)(2)(iii)(B), "Where the account involves the issuance of payment stablecoins, these terms must be consistent with paragraph (a)(2)(iv) of this section." At the end of (a)(2)(iii)(C), "and, where payment stablecoins issued to the customer remain outstanding, the actions the permitted payment stablecoin issuer will take with respect to those payment stablecoins."

The definitional sentence matters: every lawful PPSI must hold order-triggered capability as a condition of issuing (12 U.S.C. 5903(a)(6)(B)), and a lawful order names its targets "with reasonable particularity" (91 Fed. Reg. 18593). Without the distinction, the exception would swallow the rule.

6. Add § 1033.220(d) — reliance on conforming verification (safe harbor)

(d) Effect of conforming verification. Except with respect to a significant or systemic failure to implement the requirements of this section, a permitted payment stablecoin issuer that verifies the identity of a customer by means of a credential with respect to which it has performed the procedures described in paragraph (a)(2)(ii)(D) of this section, and that determines the status of the credential at the intervals its risk-based procedures specify, will be deemed to have formed and maintained the reasonable belief required by paragraph (a)(2) of this section with respect to that customer. The same effect applies to a verification performed under paragraph (a)(2)(ii)(B) of this section with respect to a customer who is unable to present such a credential, where the permitted payment stablecoin issuer has performed and recorded its non-documentary procedures.

Modeled on proposed 12 CFR 19.262(a) (91 Fed. Reg. 37840). We note § 19.262(a) binds only the OCC. Because this rule is issued jointly by FinCEN and the four primary Federal payment stablecoin regulators — the agencies state that they are "issuing a single, joint rule, ensuring consistent and uniform application of CIP requirements to all PPSIs subject to each Agency's jurisdiction" (91 Fed. Reg. 37236) — a corresponding provision in 31 CFR part 1033 would provide a consistent standard across all five agencies' supervision of PPSIs. We invite the agencies to confirm that effect expressly in the final rule.

7. Amend § 1033.220(a)(2)(ii)(B)(2) — conjunction

Replace "and" with "or" before the final circumstance, conforming the codified text to the preamble at 91 Fed. Reg. 37242 and Table 3 at 91 Fed. Reg. 37252.
