ALTER MERIDIAN PTY LTD T/A TRUE ALTER, BLAKE MORRISON

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C24

Submitter Information

Organization Name: Alter Meridian Pty Ltd T/A True Alter

Organization Type: Company

Name: Blake Morrison

Submitted Date: 08/20/2026

This comment addresses Questions 5, 6 and 7. The full comment is provided in the attached PDF.

Alter Meridian Pty Ltd builds identity infrastructure. We are not a permitted payment stablecoin issuer, are not seeking to become one, and take no position on the rule's treatment of stablecoin issuance. We build the class of mechanism Questions 5 and 6 concern and so hold a commercial interest in how they are resolved, and state it at the outset.

Question 5.
The text should address digital identity, expressed as properties a method must exhibit rather than as a list of technologies. The agencies' own reason for declining text, that these tools "vary in how they operate and in their trustworthiness" (91 Fed. Reg. 37,242, cols. 1-2), argues against naming products and standards, which are stale before a rule is final. It is no argument against text, because the property distinguishing a trustworthy method from an untrustworthy one stays stable as the tools change. Declining to write text is not neutral. It moves the decision to the examination room, and Treasury's March 2026 report to Congress recorded institutions naming the absence of explicit guidance, and apprehension of adverse examiner feedback, among the barriers to adoption.

We suggest four properties. (a) The credential can be checked independently of the party that produced it, the shape the proposal already requires of non-documentary methods (id. at 37,271, col. 2). (b) It identifies the party that made the underlying assertion, since an institution cannot assess trustworthiness it cannot see. (c) Its currency can be determined, and it can be withdrawn. (d) The person it describes can see that it was presented, and to whom. Each is testable and none names a vendor, a protocol or a standards body.

The proposal's distinction between a state-issued mobile ID under proposed section 1033.220(a)(2)(ii)(A) and a non-government credential treated as a non-documentary method should survive into the text. Collapsing it toward documentary treatment makes government issuance a practical precondition. Collapsing it the other way discards the assurance a government issuer carries.

Question 6.
The benefit is reach. The proposal requires procedures for the person who "is unable to present an unexpired government-issued identification document" (id. at 37,271, col. 2), which describes a substantial population, not principally a digital-asset one. Our test for any scheme, our own included, is whether the person who cannot produce the document is better off under it. The second benefit is reduced exposure, since a method returning a result without transferring the underlying attributes leaves less to retain for the five years this rule requires after an account closes, and less to expose in a breach.

The principal risk is economic rather than technical. Where a verification provider's revenue rises with the volume and richness of the data it can supply, its incentive is to collect more, hold it longer, and widen the set of parties it supplies. Privacy-preserving cryptography changes what travels on the wire and leaves that incentive intact. Our own company is compensated the other way, so we are not disinterested here, and the risk holds regardless of who addresses it. Any property-based text should ask whether a method requires the underlying data to be concentrated in a third party in order to function. Two further risks. Relayed assurance, where a weak original assertion is relayed through a well-engineered wrapper and arrives looking strong, mitigated by property (b). And silent exclusion, where an automated method fails without an explanation the person can act on, mitigated by preserving a human-reviewed path.

Question 7.
We have no basis on which to estimate frequency. One structural point should be explicit. Proposed section 1033.220(a)(6) permits reliance only on another financial institution that is subject to an AML/CFT programme rule and regulated by a Federal functional regulator, under contract, with annual

certification. No digital identity credential provider satisfies that description, and we do not expect one to. A PPSI using such a credential is therefore not relying on the provider under (a)(6), but applying a non-documentary method under section 1033.220(a)(2)(ii)(B), with the CIP obligation remaining entirely its own. That allocation is correct and the text should say so. The clarity the digital identity path requires belongs in (a)(2)(ii)(B), not in (a)(6).

Blake Morrison, Director, Alter Meridian Pty Ltd T/A True Alter, legal@truealter.com

From: Blake Morrison, Director, Alter Meridian Pty Ltd T/A True Alter

To: 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. 37,234; FinCEN Docket FINCEN-2026-0101 / RIN 1506-AB74; OCC-2026-0331; Docket No. R-1885 / RIN 7100-AH18; RIN 3064-AG28; NCUA-2026-0793

We write in response to the request for comment and address Questions 5, 6 and 7.

Our Interest

Alter Meridian Pty Ltd builds identity infrastructure. We are not a permitted payment stablecoin issuer, we are not seeking to become one, and we take no position on the rule's treatment of stablecoin issuance. Our interest is narrower and we state it at the outset, because we build the class of mechanism Questions 5 and 6 concern and therefore hold a commercial interest in how those questions are resolved. We have written this comment so that it remains useful whether or not the answer favours us.

Summary

I. **Write text, but write properties rather than named technologies.**
The agencies' own stated reason for declining text, that these tools "vary in how they operate and in their trustworthiness," is an argument against enumerating tools rather than an argument for silence.

II. **The most significant risk lies in the economics that sustain a credential rather than in the credential itself.**
A verification method whose provider is compensated in proportion to the data it holds will accumulate data, whatever cryptography sits on the wire.

III. **Question 7 exposes a structural point the text should make explicit.**
A credential provider cannot be a reliance party under proposed § 1033.220(a)(6) and should not be treated as one, and the clarity the digital identity path requires belongs instead in § 1033.220(a)(2)(ii)(B).

<u>Question 5.</u> Should the regulatory text explicitly discuss digital identity solutions or verifiable credentials?

Yes, expressed as properties a method must exhibit rather than as a list of technologies.

The proposal supplies its own reason for doing so. The agencies observe that digital identity tools "vary in how they operate and in their trustworthiness," (91 Fed. Reg. 37,242, cols. 1-2) and conclude that such variation is best accommodated by maintaining flexibility. We accept the observation. The conclusion does not follow from it, because that variation is a strong case against naming products or standards in the text, where any such list is stale before the rule is final, and no case at all against text itself, where the property distinguishing a trustworthy method from an untrustworthy one remains stable even as the tools change.

Declining to write text is not a neutral act. It relocates the decision from the rule to the examination room, where an institution's willingness to use a non-documentary method turns on its supervisor's appetite rather than on anything it can read in advance. Treasury's March 2026 report to Congress recorded precisely this dynamic, in which institutions named the absence of explicit guidance that digital identity is an allowable CIP form, together with apprehension of adverse examiner feedback, among the barriers to adoption. Declining to write text preserves that barrier rather than removing it.

We suggest the text describe what a digital identity credential must achieve, in terms the agencies already employ elsewhere in the proposal. A credential may support a reasonable belief as to a customer's true identity where:

a) **It can be checked independently of the party that produced it.**
   The proposal already requires this shape for non-documentary methods, describing verification "through the comparison of information provided with respect to the customer with information obtained from a consumer reporting agency, public database, or other source" (id. at 37,271, col. 2). A credential validated only by asking the party that issued it is a reference rather than a verification.

b) **It identifies the party that made the underlying assertion.**
   The variation the agencies named is variation in trustworthiness, and an institution cannot assess trustworthiness it cannot see. A credential presenting a conclusion while concealing whose judgement produced it forecloses the risk-based assessment the rule requires.

c) **Its currency can be determined, and it can be withdrawn.**
   The institution should be able to establish that the assertion remains good at the moment of reliance, and the party that made the assertion should be able to withdraw it. An assertion that cannot be withdrawn is permanent, whatever risk assessment produced it.

d) **The person it describes can see that it was presented, and to whom.**
   The property is ordinarily framed as a privacy protection, though it operates equally as a control.

Each property is testable and none of them names a vendor, a protocol or a standards body. They would still mean something in ten years.

The proposal already draws a distinction we think should survive into the text. A state-issued mobile ID or driver's licence may constitute an "unexpired government-issued identification" under proposed § 1033.220(a)(2)(ii)(A) (id. at 37,271, col. 2), while a non-government privacy-preserving credential may instead be a non-documentary method. Keeping those categories separate matters. Collapsing them in

the direction of documentary treatment would render government issuance a practical precondition, which defeats the purpose of the non-documentary path, while collapsing them in the other direction would discard the assurance a government issuer actually carries.

Question 6. What are the benefits and risks?

6a) Benefits

The material benefit is reach. The proposal requires a PPSI's non-documentary procedures to address the case where an individual "is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard" (id. at 37,271, col. 2). That describes a substantial population which is not principally a digital-asset population, comprising people whose documents have lapsed or were never issued, those who have moved between jurisdictions, those paid outside institutional systems, and the young, who have had no time to accumulate a documentary record.

We apply one test to any proposal in this space, our own included. Where a credential scheme in practice works only for a person who already holds a strong government document, it has not solved reachability but has added a step for people who were never excluded. We would encourage the agencies to ask, of any method offered under this rule, whether the person who cannot produce the document is better off under it.

The second benefit is reduced exposure. A method returning a verification result without transferring the underlying attributes means the institution holds less, which matters under this rule specifically, since the proposal requires identifying information to be retained for five years after the account is closed. Information never collected cannot be held for those five years, and cannot be exposed when the institution is breached.

6b) Risks

The accumulation incentive. Treasury's March 2026 report recorded the concern that identity solutions may themselves become large repositories of personal information. We share that concern, and we think the mechanism is economic rather than technical. Where a verification provider's revenue rises with the volume and richness of the data it can supply to verifiers, its incentive is to collect more, retain it longer, and widen the set of parties it can supply. Privacy-preserving cryptography does not alter that incentive; it alters what travels on the wire while leaving the provider's reason to accumulate intact. A regime crediting the cryptography without examining the incentive will approve architectures that concentrate data by design.

The durable answer is a method whose economics do not require accumulation in order to function, where the person being verified is the party compensated when their identity is read and the provider's revenue does not scale with how much it holds about them. Our own company operates that model, so we are not a disinterested observer of this point. We raise it because the agencies asked for risks and because the risk holds regardless of who addresses it, our own participation included. Where the agencies write any property-based text, we would encourage them to include the question of whether a method requires the underlying data to be concentrated in a third party in order to function.

Relayed assurance. A credential presents as a single assertion while resting on a chain of earlier ones. Where that chain is not visible, a weak original assertion can be relayed through a well-engineered wrapper and arrive looking strong. The concern arises from ordinary practice, since identity systems are composed from parts each designed to be trusted only at its own boundary. The second property above, that a credential identify the party behind the assertion, is the mitigation, and it costs little.

Silent exclusion. An automated identity method that fails for a person usually fails without an explanation the person can act upon, and often without a route to contest it. Where the agencies bring digital identity into CIP, we would encourage them to preserve the customer's access to a human-reviewed verification path, since a non-documentary method that becomes the only path reproduces, in a new form, the exclusion the non-documentary path exists to relieve.

Question 7. Likelihood of reliance on another PPSI's or federally regulated institution's CIP

We have no basis on which to estimate frequency and defer to institutions that do. One structural point should be explicit whatever the frequency proves to be.

Proposed § 1033.220(a)(6) permits reliance only on another financial institution that is subject to an AML/CFT programme rule and regulated by a Federal functional regulator, under contract, with annual certification that it has implemented that programme. No digital identity credential provider satisfies that description, and we do not expect one to.

It follows that a PPSI using a digital identity credential is not relying on the provider within the meaning of (a)(6), but is applying a non-documentary method under § 1033.220(a)(2)(ii)(B), and the CIP obligation remains entirely with it. That allocation is correct and we support it. We suggest the text say so. The alternative reading, that a credential provider is a reliance party, would imply an expectation of federal functional regulation that no such provider carries, and would deter institutions from using a method the agencies have said they are open to.

The clarity the digital identity path requires is therefore not in (a)(6) but in (a)(2)(ii)(B), confirming that a digital identity credential meeting stated properties is available as a non-documentary method, and that the PPSI's own responsibility is undiminished by using one.

We would be glad to expand upon any of the above, or to answer questions.

Respectfully submitted,

Blake Morrison
Director

Alter Meridian Pty Ltd T/A True Alter
ACN: 696 662 049 / ABN: 54 696 662 049
Queensland, Australia
legal@truealter.com