NICO PAULO MENDOZA

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C03

Submitter Information

Name: Nico Paulo Mendoza

Submitted Date: 07/21/2026

This comment responds principally to Questions 5, 6, and 8 of the notice, concerning digital identity, verifiable credentials, and their benefits, risks, and role in innovation.

I recommend that the customer-identification records the rule requires be captured in discrete, machine-readable fields, with the source, method, date, and result of verification recorded alongside them, using publicly documented data standards and without mandating any particular messaging format. I further recommend that the Legal Entity Identifier (LEI) be permitted as a supplementary entity identifier and as a non-documentary verification source, without displacing the taxpayer identification number the rule requires.

I propose specific implementing language, and provide technical illustrations of structured identity records, U.S. identifier validation methods, and verification-provenance recordkeeping, in the attached comment.

Submitted in an individual capacity by Nico Paulo I. Mendoza, independent advisor in payment and financial market infrastructure. The views expressed are my own and do not represent any institution.

Nico Paulo I. Mendoza

Independent advisor, payment and financial market infrastructure

Public comment on the Notice of Proposed Rulemaking

Permitted Payment Stablecoin Issuer Customer Identification Program

Docket No. FINCEN-2026-0101, submitted via regulations.gov

This comment responds principally to Questions 5, 6, and 8 of the notice, concerning digital identity, verifiable credentials, and their benefits, risks, and role in innovation. I submit it in an individual capacity as an independent advisor in payment and financial market infrastructure; the views are my own and do not represent any institution.

Summary of recommendation

I respectfully request that the agencies, in implementing the customer-identification-program requirement, and in particular the retention of the methods and results of non-documentary verification at proposed § 1033.220(a)(3), take the following steps:

1. **Express the recordkeeping expectation in structured terms.** Identity information should be preserved in discrete, machine-readable fields rather than free text.
2. **Require that records capture the provenance of verification**, the source, method, date, and result of verification, and the resolution of any material discrepancy.
3. **Permit the Legal Entity Identifier (LEI) as a supplementary entity identifier and as a non-documentary verification source**, without displacing the taxpayer identification number the rule requires.

Each recommendation is technically neutral: it references openly published data standards as acceptable means, and mandates no messaging format or proprietary platform.

Suggested regulatory language (§ 1033.220(a)(3))

> *Records should preserve identifying information in discrete, machine-readable fields, and should record the verification source, method, date, and result, and the resolution of any substantive discrepancy. Publicly documented data standards may be used for this purpose; no particular messaging standard is required.*

1. Structured identity records serve the rule's purpose (Questions 5, 6)

A customer-identification program exists so that identity information can be used, screened against U.S. sanctions and watchlists, reconciled against records, and matched to information that accompanies a transfer. Free-text identity data is a material source of screening and reconciliation failures, because it forces reliance on probabilistic ("fuzzy") matching that adversaries exploit through transliteration, truncation, and field misplacement. Capturing each element in a discrete, labeled field enables reliable, field-level comparison.

Structure is not a complete solution, and I do not suggest it is: names still require transliteration, alias, and similarity controls even when stored in discrete fields. What structure removes is the avoidable failure that

unstructured data introduces, the conflation of distinct elements into a single text field that no screening or reconciliation process can reliably parse. The customer-identification data a program collects can be mapped to compatible, openly published payment-message fields, so that identity captured at onboarding is expressed the same way as the party data used elsewhere in the payment lifecycle.

The regulatory text or accompanying guidance should expressly recognize digital identity solutions and verifiable credentials as permissible non-documentary methods, without mandating a particular credential or technical architecture. Their potential benefits include evidence integrity, reusable verification, selective disclosure, provenance, and reduced re-keying. Risks include weak or compromised credential issuers, stale or unrevoked credentials, privacy and correlation harms, exclusion of persons unable to obtain credentials, vendor concentration, and false assurance. PPSIs should therefore evaluate issuer trust, assurance level, expiration and revocation status, binding to the customer, and cryptographic verification results, while applying data-minimization and access controls.

2. Recording the provenance of verification (Question 6; § 1033.220(a)(3))

The proposal already requires that the methods and results of non-documentary verification be retained. That requirement is best served if the record captures, in structured form, whether an identifier was verified, against which source and authority, by what method, when, and how any discrepancy was resolved, rather than as a free-text case note. Structured verification provenance is what lets a supervisor or screening system rely on the record programmatically. It also makes the absence of verification visible: where an identifier cannot be independently checked, a structured record shows that plainly, which is itself a risk indicator the agencies and issuers can act on.

3. The LEI as a supplementary, verifiable entity identifier (Question 8)

The proposal requires a U.S. taxpayer identification number for entity customers. Nothing in this recommendation would change that requirement. I recommend only that the Legal Entity Identifier be permitted in addition, as a supplementary identifier and as a non-documentary verification source, for one reason: it is a globally standardized identifier (ISO 17442) whose record and status can be checked electronically against the publicly available GLEIF Global LEI Index. EIN/name combinations do not have a generally available nationwide public lookup.

The limits of each source should be stated honestly, and the rule should reflect them:

1. **LEI validation** confirms that an LEI record exists and its registration status; it does not replace entity-formation documents, beneficial-ownership determination, or broader customer verification.
2. **IRS TIN-Matching** confirms that a name and taxpayer identification number correspond, for eligible users; it does not independently establish complete legal identity.
3. **Consent-based SSA verification** checks whether submitted attributes match SSA records; it does not verify identity.

Recognizing the LEI as a supplementary, independently verifiable data point, recorded together with its verification provenance, strengthens the identity record without displacing any field the rule requires, and without mandating that any customer obtain one.

4. Technical neutrality and proportionality

The recommendation is outcome-based. It asks the agencies to reference openly published data standards as acceptable means of structuring and verifying identity data, while leaving implementation to the issuer and mandating no messaging format or proprietary platform. This preserves flexibility and proportionality for smaller issuers, while ensuring that the identity data a customer-identification program produces is portable, screenable, and verifiable rather than locked in free text.

Respectfully submitted,

Nico Paulo I. Mendoza
Independent advisor, payment and financial market infrastructure

EXHIBIT

Illustrative structured representations

Supporting the recommendation above. Illustrative and technical; not a normative usage guideline.

> *All names, addresses, and identifiers below are fictitious and are constructed to be invalid on purpose (for example, an SSN in a range the Social Security Administration never issues, and placeholder EIN and LEI values); they must not be treated as real. Element names follow the publicly published ISO 20022 data dictionary. No proprietary usage guideline or copyrighted text is reproduced.*

A. Minimum identity fields, mapped to structured elements

The rule's minimum fields for a customer are name; date of birth (for an individual) or date of formation (for an entity); address; and an identification number. These map to discrete, openly published ISO 20022 fields. Place of birth and similar attributes are not minimum fields and, where collected, are optional or risk-based.

```
<!-- entity customer: minimum fields, structured -->
<Cdtr>
  <Nm>Acme Holdings LLC</Nm>
  <PstlAdr>
    <Dept>Suite 300</Dept>
    <StrtNm>Market Street</StrtNm>
    <BldgNb>500</BldgNb>
    <PstCd>94105-1234</PstCd>
    <TwnNm>San Francisco</TwnNm>
    <CtrySubDvsn>CA</CtrySubDvsn>
    <Ctry>US</Ctry>
  </PstlAdr>
  <Id><OrgId>
    <Othr><Id>00-0000000</Id><SchmeNm><Cd>TXID</Cd></SchmeNm><Issr>US</Issr></Othr>
    <LEI>5493000FAKEUS0LEI001</LEI>   <!-- supplementary, verifiable -->
  </OrgId></Id>
  <!-- date of formation retained in the issuer's identity record -->
</Cdtr>
```

The taxpayer identification number (TXID) is the required identifier; the LEI is supplementary. "Date of formation" is a minimum field for an entity and is retained in the identity record. Identifiers are fictitious.

B. A U.S. natural person

```
<Dbtr>
  <Nm>Jane A Doe</Nm>
  <PstlAdr>
    <Dept>Apt 5B</Dept>
    <StrtNm>Elm Street</StrtNm>
    <BldgNb>1420</BldgNb>
    <PstCd>78701-0100</PstCd>
    <TwnNm>Austin</TwnNm>
    <CtrySubDvsn>TX</CtrySubDvsn>
    <Ctry>US</Ctry>
  </PstlAdr>
  <Id><PrvtId>
    <DtAndPlcOfBirth>
      <BirthDt>1988-03-22</BirthDt>   <!-- minimum field -->
      <CityOfBirth>Denver</CityOfBirth>   <!-- optional / risk-based -->
      <CtryOfBirth>US</CtryOfBirth>
    </DtAndPlcOfBirth>
    <Othr><Id>900-00-0000</Id><SchmeNm><Cd>SOSE</Cd></SchmeNm><Issr>US</Issr></Othr>
  </PrvtId></Id>
</Dbtr>
```

Date of birth is a minimum field; place of birth is shown as optional/risk-based. SchmeNm uses the published external person-identification code list (SOSE, TXID, CCPT, DRLC). 900-00-0000 is deliberately invalid, the SSA never issues 900-series area numbers, so it is neither a real SSN nor a valid ITIN.

C. A structured verification-provenance record

The record below is illustrative structure an issuer would retain to satisfy the requirement to keep the method and result of verification. The element names are illustrative, this is not a standardized message element, but the point is that verification provenance should be structured and required.

```
<IdentityVerificationRecord>              <!-- illustrative; issuer-retained -->
  <Party>Acme Holdings LLC</Party>
  <Identifier>5493000FAKEUS0LEI001</Identifier>
  <IdentifierType>LEI</IdentifierType>
  <Verified>true</Verified>
  <VerificationSource>GLEIF Global LEI Index</VerificationSource>
  <VerificationMethod>reference-data lookup</VerificationMethod>
  <VerificationDate>2026-08-10</VerificationDate>
  <Result>active</Result>
  <DiscrepancyResolution>none</DiscrepancyResolution>
</IdentityVerificationRecord>
```

A parallel record for a taxpayer identification number would honestly read Verified=limited, Source=IRS TIN-Matching (eligible filers only), signaling that the identifier was confirmed only as a name/number match, not independently proofed. That visible difference is a risk indicator the rule can act on.

D. Note on the address structure

The address fields above are presented as one illustrative U.S. implementation profile, not as a universal mapping. In this profile the primary street number is carried in BldgNb (the ISO element for a street/house number), and the USPS secondary-unit designator (suite, apartment) is carried in Dept, with SubDept for a further nested unit; some implementations instead use a unit-specific or physical-location element. U.S. domestic address components (street, secondary unit, city, two-letter state, ZIP+4) can be captured in discrete fields consistent with United States Postal Service addressing conventions; the readable spellings shown are for clarity and are not offered as postal-abbreviation output.

Reference standards and programs

ISO 20022 (party-identification and postal-address components); ISO 17442 (Legal Entity Identifier); ISO 3166 (country codes). GLEIF and accredited issuing organizations (LEI reference data / lookup). IRS TIN-Matching (name/TIN correspondence, eligible filers). Consent-based Social Security Administration verification. United States Postal Service addressing conventions. Bank Secrecy Act recordkeeping requirements. Fedwire Funds Service and FedNow Service ISO 20022 implementations.

Prepared and submitted by Nico Paulo I. Mendoza, independent advisor, payment and financial market infrastructure, in an individual capacity.