America's Credit Unions

# Regulatory Comment: Permitted Payment Stablecoin Issuer Customer Identification Program

## THE ISSUE:

On June 22, 2026, the Financial Crimes Enforcement Network (FinCEN); the Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System (FRB); the Federal Deposit Insurance Corporation (FDIC); and the National Credit Union Administration (NCUA) published a Joint Notice of Proposed Rulemaking (NPRM) that requires permitted payment stablecoin issuers (PPSIs) to maintain an effective customer identification program (CIP).

## IMPACT TO CREDIT UNIONS:

The NPRM does not directly regulate credit unions. However, PPSIs can leverage parent credit unions' existing CIP programs, but only if such programs cover PPSI-specific risks and implement the Bank Secrecy Act (BSA)/CIP requirements applicable to both entities. In this case, credit union parent companies may need to modify or expand existing CIP programs to cover applicable requirements specific to PPSI activities, such as issuing or redeeming a payment stablecoin; managing related reserves; and providing custodial or safekeeping services for stablecoins, reserves, or private keys. Further, parent credit unions will need to properly allocate CIP responsibilities between the parent credit union and the subsidiary PPSI and avoid any gaps or duplication.

## KEY POINTS:

- The CIP requirements under this NPRM are similar to existing CIP requirements for credit unions and other financial institutions under existing FinCEN rules, but with a potential addition of requirements that reflect PPSI stablecoin activities.
- The NPRM does not prescribe a one-size-fits-all approach to CIP.
- Rather, the NPRM directs a PPSI's CIP to address the types of accounts it intends to maintain, how it allows those accounts to be opened, and the types of identifying information available.
- The NPRM proposes adding a new definition of "account" which resembles how "account" is defined in other CIP rules, but contains unique provisions that reflect the kinds of activities in which PPSIs can engage, such as issuing or redeeming a payment

stablecoin; managing related reserves; and providing custodial or safekeeping services for stablecoins, reserves, or private keys.

## ACTION NEEDED: Deadlines and contacts

Please use the comment link below to respond to America's Credit Unions' survey. This will help shape the discussion and better address your needs in our comment letters.

- Comments due to America's Credit Unions: August 7, 2026 — **Submit here**.
- Comments due to FinCEN: August 21, 2026
- Questions? Contact Jeremy Greenberg, Regulatory Advocacy Counsel, Innovation & Technology, America's Credit Unions
- Agency contacts: FinCEN, Regulatory Support Section; OCC, Kenneth Kohrs, BSA/AML Lead Expert, Office of the Chief National Bank Examiner; Jina Cheon, Assistant Director, Melissa Lisenbeen, Counsel, or Henry Barkausen, Counsel, Bank Advisory Group, Chief Counsel's Office, (202) 649-5490.

## QUESTIONS TO CONSIDER:

1. Should any CIP requirement be extended to secondary market activity (e.g., a holder of stablecoin transacting directly on a blockchain without the involvement of a PPSI)? If not, why not? If so, in what circumstances?
2. Should the NPRM be clarified or refined to account for situations where a customer's only desired relationship with a PPSI is to redeem a payment stablecoin? Why or why not?
3. What, if anything, could be changed to make the NPRM more conducive to industry innovation? Explain why any changes would positively or negatively impact PPSIs', or their parent credit unions', expected operations and illicit financial risk to the U.S. financial system.
4. Should the regulatory text explicitly discuss digital identity solutions or verifiable credentials as part of verifying customer's identities? Why or why not?

## BACKGROUND:

The NPRM implements the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) directives to treat PPSIs as financial institutions for purposes of the BSA to require such PPSIs to maintain an "effective customer identification program, including identification and verification of account holders."[1]

In September 2025, Treasury issued an advanced notice of proposed rulemaking (ANPRM) that sought public comment on potential Treasury regulations implementing the GENIUS Act, including those imposing BSA anti-money laundering (AML), countering the financing of terrorism (CFT), and sanctions compliance program obligations. In response to the ANPRM, Treasury received comments from stakeholders including credit unions, banks, stablecoin issuers, digital asset exchanges, and other groups. Treasury reviewed and considered pertinent comments in crafting this NPRM.

In April 2026, FinCEN issued a separate NPRM (PPSI AML/CFT NPRM) that proposed changes to its existing regulations to apply BSA obligations to PPSIs, which addressed compliance programs, reporting, recordkeeping, and other GENIUS Act requirements. Further, the PPSI AML/CFT NPRM added several new definitions that arose from the GENIUS Act.

## SECTION-BY-SECTION ANALYSIS

A. Proposed 31 CFR 1033.100 – Definitions

31 CFR 1033.100(A) – *Account*

- "A formal relationship between a PPSI and a customer, established to provide or engage in services, dealings, or other financial transactions."
- An illustrative list of activities that may fall within "services, dealings, or other financial transactions" includes:
    - Issuing or redeeming a payment stablecoin;
    - Managing related reserves, including purchasing, selling, and holding reserve assets or providing custodial services for reserve assets;
    - Providing custodial or safekeeping services for payment stablecoins, required reserves, or private keys of payment stablecoins;
    - Other activities that directly support the above list of activities; or
    - Providing services of a digital asset provider that are authorized by the primary Federal payment stablecoin regulator or the State payment stablecoin regulator, as applicable.
- An individual with no established relationship with a PPSI could hold a PPSI's product, specifically a payment stablecoin, and then seek to engage directly with a PPSI for a financial service, making them a PPSI customer with an account.

[1] See 12 U.S.C. § 5903(a)(5)(A)9v); see also 31 U.S.C. § 5318.

- Instances where an activity does not form an account relationship:
    - Where a formal relationship is not established with a person, such as payment stablecoin activity that does not directly involve the PPSI as a party to the transaction other than via a smart contract; or
    - Ownership or control of a PPSI's payment stablecoins alone, without other indicators of a formal relationship.
- "Account" does not include an account that the PPSI acquires through an acquisition, merger, purchase of assets, or assumption of liabilities from a financial institution regulated by a Federal functional regulator or an account opened for the purpose of participating in an employee benefit program under the Employee Retirement Income Security Act of 1974 (ERISA).

31 CFR 1033.100(B) – *Customer*

i. A person that opens a new account; and

ii. An individual who opens a new account for:

A. An individual who lacks legal capacity, such as a minor; or

B. An entity that is not a legal person, such as a civic club.

- A "customer" does not include:

    i. A financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator;

    ii. A person described in § 1020.315(b)(2) through (4) of 31 CFR chapter X (listing transactions of exempt persons);

    iii. A person that has an existing account with the PPSI, provided the PPSI has a reasonable belief that it knows the true identity of the person; or

    iv. A person acquiring or redeeming a payment stablecoin from a means other than directly from or directly to the PPSI.

- Transfers of payment stablecoins on the secondary market do not make a party to the transfer a customer of a PPSI.

31 CFR 1033.100(C) – *Digital Asset Service Provider*

- Any individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated that, for compensation or profit, engages in business in the U.S. (including on behalf of customers or users in the U.S.) of:

    A. Exchanging digital assets for monetary value;

    B. Exchanging digital assets for other digital assets;

    C. Transferring digital assets to a third party;

    D. Acting as a digital asset custodian; or

    E. Participating in financial services related to digital asset insurance.

- A "digital asset service provider" does not include:

i. A distributed ledger protocol;

ii. Developing, operating, or engaging in the business of developing distributed ledger protocols or self-custodial software interfaces;

iii. An immutable and self-custodial software interface;

iv. Developing, operating, or engaging in the business of validating a transaction or operating a distributed ledger; or

v. Participating in a liquidity pool or other similar mechanism for the provisioning of liquidity for peer-to-peer transactions.

- The meaning of "distributed ledger protocol" is defined by 12 USC 5901(9):
    - Publicly available and accessible executable software deployed to a distributed ledger, including smart contacts or networks of smart contracts.

B. Proposed 31 CFR 1033.220(A)(2) – Identity Verification Procedures

- Requires that the CIP includes risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable.
- The procedures must be based on the PPSI's assessment of the relevant risks, including those presented by the various types of accounts maintained by the PPSI, the methods of opening accounts provided by the PPSI, the types of identifying information available, and the PPSI's size, location, and customer base.

I. 31 CFR 1033.220(a)(2)(i)

- PPSIs must obtain from each customer the following information prior to opening an account:
    - 1. Name;
    - 2. Date of birth, for an individual; or date of formation, for a person that is not an individual;
    - 3. Address, a residential and mailing address for individual; or the principal place of business, local office, or other physical address and mailing address for a person other than an individual; and
    - 4. Identification number.
- If an individual does not have a residential or business address, the individual may provide an Army Post Office or Fleet Post Office box number of the residential or business street address of a next to kin or another contact individual.
- If the customer is a corporation, partnership, or trust, it must provide the address of its principal place of business, local office, or other physical location.
    - A Post Office box (PO Box) is not acceptable for these purposes.
    - A virtual address, or an address that is not a physical location, is not acceptable for these purposes.
- Identification numbers for U.S. persons are taxpayer identification numbers. For non-U.S. persons, the identification number can be one or more of the following:

    - A taxpayer identification number;
    - Passport number and country of issuance;
    - Alien identification card number; or
    - Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
- For a non-U.S. person that is not an individual and that does not have an identification number, the PPSI must request alternative government-issued documentation clarifying the existence of the person.
- There is an exception to the above requirements for persons applying for a taxpayer identification number.
    - Such an exception requires that the CIP includes procedures for confirming that the application for a taxpayer identification number was filed, as well as obtaining the taxpayer identification number within a reasonable period of time after the account is opened.

II. 31 CFR 1033.220(A)(2)(II) – Customer Verification

- Requires that the CIP contains procedures for verifying the identity of each new customer within a reasonable period of time after the customer's account is opened.
- Procedures must describe when the PPSI will use documents, non-documentary methods, or a combination of both methods for customer verification.

A. 31 CFR 1033.220(A)(2)(II)(A) – Verification Through Documents

- If the PPSI is relying on documents to verify a customer's identity, then the CIP must contain procedures that set forth the documents that the PPSI will use.
- For an individual, a PPSI can use an unexpired government-issued identification evidencing nationality or residence that contains a photograph or similar safeguard, such as a driver's license or passport.
- For a person other than an individual, the document must show the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

B. 31 CFR 1033,220(A)(2)(II)(B) – Verification Through Non-Documentary Methods

- The CIP must contain procedures that set forth the non-documentary methods the PPSI will use. These methods include:
    - Contacting a customer;
    - Independently verifying the customer's identity through the comparison of information provided with respect to the customer with information obtained from a customer reporting agency, public database, or other source;

    - Checking references with other financial institutions; or
    - Obtaining a financial statement.
- A PPSI's non-documentary procedures are required to address situations where an individual is:
    - Unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard;
    - The PPSI is not familiar with the documents presented;
    - The account is opened without obtaining documents;
    - The customer opens the account without meeting in person; or
    - The PPSI is otherwise presented with circumstances that increase the risk that the PPSI will be unable to verify the true identity of a customer through documents.

C. 31 CFR 1033.220(A)(2)(II)(C) – Additional Verification of Certain Customers

- A PPSI's CIP must address how the PPSI—based on the PPSI's risk assessment of a new account opened by a customer that is not an individual—will obtain information about individuals with authority or control over such account to verify the customer's identity.
- This verification method applies only when a PPSI cannot verify the true identity of a customer that is not an individual through either documentary or non-documentary methods.

III. 31 CFR 1033.220(A)(2)(III) – Lack of Verification

- In the case that a PPSI cannot form a reasonable belief that it knows the true identity of a customer, procedures are required to describe:
    1. When the PPSI should not open an account;
    2. The terms under which a customer may use an account while the PPSI attempts to verify the customer's identity; and
    3. When the PPSI should file a Suspicious Activity Report (SAR) in accordance with applicable law and regulation.

3. 31 CFR 1033.220(A)(3) – Records

- The CIP must include procedures for making and maintaining a record for all information obtained by the PPSI through the CIP.
- Section 1033.220(a)(3)(i) requires the records to include:
    1. All identifying information about a customer obtained under the CIP;
    2. A description of any document relied on to verify the identity of the customer under the CIP, noting: 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;

3. A Description of the methods and results of any measures undertaken to verify the identity of a customer; and

4. A description of the resolution of each substantive discrepancy discovered when verifying the identifying information.

- A PPSI must retain the identification about a customer obtained under § 1033.220(a)(3)(i)(A) for five years after the date the account is closed and the information regarding the verification of a customer's identity records collected under § 1033.220(a)(3)(i)(B), (C), and (D) for five years after the record is made.

4. 31 CFR 1033.220(A)(4) – Comparison with Government Lists
- A PPSI's CIP is required to include reasonable procedures for determining whether a customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators.
- The procedures require PPSIs to follow all Federal directives issued in connection with such lists.
- PPSIs are to receive a separate notification regarding the lists that must be consulted for the purposes of this provision.
- Failure to comply with requirements associated with such lists may result in criminal or civil penalties.

5. 31 CFR 1033.220(A)(5) – Customer Notice
- The CIP must include procedures for providing customers with adequate notice that the PPSI is requesting information to verify their identities.
- Notice is considered adequate if the PPSI generally describes the identification requirements of this section and provides notice in a manner reasonably designed to ensure that a prospective customer is able to view the notice, or is otherwise given notice, before opening the account.

6. 31 CFR 1033.220(A)(6) – Reliance on Another Financial Institution
- A PPSI's CIP may include procedures specifying when a PPSI may rely on another Federally regulated financial institution's performance of a procedure with respect to any PPSI customer that is opening or has opened an account.
- Such reliance would have to be reasonable under the circumstances, and the other financial institution on which the PPSI seeks to rely must be subject to an AML/CFT program with CIP requirements, as well as regulated by a Federal functional regulator.
- Institutions must have a contract requiring the institution on which the PPSI seeks to rely to certify annually to the PPSI that it has implemented an AML/CFT

program and will perform (or its agent will perform) the specified requirements of the PPSI's CIP.

- This provision does not change a PPSI's CIP obligation, and the PPSI would remain responsible for its compliance.

C. 31 CFR 1033.220(b) – Exemptions

- The appropriate Federal functional regulator, with the concurrence of the Secretary, may by order of regulation, exempt any PPSI or any type of account from the requirements of this section.
- The Secretary, with the concurrence of the Federal functional regulator, may exempt any PPSI or any type of account from the requirements of this section.
- In issuing such exemptions, the Federal functional regulator and the Secretary must consider whether the exemption is consistent with the purposes of the BSA, safety and soundness, and the public interest.
- A Federal functional regulator and the Secretary are permitted to consider other necessary and appropriate factors.

D. 31 CFR 1033.220(c) – Other Requirements Unaffected

- Nothing in § 1033.220 relieves a PPSI of its obligation to comply with any other provision of 31 C.F.R. Chapter X (the FinCEN regulations implementing the BSA), including provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction, including requirements to have the technology capability to comply with the terms of any lawful order.

E. Compliance Date

- The rule is effective 12 months after issuance of the final rule.

### Additional Questions for Public Comment:

1. Should FinCEN and the Agencies refine or clarify its definitions of account, customer, or digital asset service provider? Are additional definitions needed?

2. Should FinCEN and the Agencies retain "formal relationship" as part of the definition of account? What are the hallmarks of a "formal relationship" between a PPSI and a user? Should FinCEN and the Agencies provide examples or attributes of a formal relationship in guidance? Would other concepts be a better foundation for the "account" definition, such as a contractual or business relationship? If so, why?

3. What are the benefits and risks of using digital identity solutions or verifiable credentials as part of verifying customers' identities?

4. What is the expected likelihood that a PPSI would rely on another PPSI's CIP or the CIP of another Federal functionally regulated financial institution's CIP?