America's Credit Unions

Regulatory Comment: Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism and Sanctions Compliance Program Requirements

THE ISSUE:

On April 10, 2026, the Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) jointly issued a notice of proposed rulemaking (NPRM) on implementing provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act's (GENIUS Act). The NPRM implements the GENIUS Act's directive to treat permitted payment stablecoin issuers (PPSIs) as financial institutions for purposes of the Bank Secrecy Act (BSA), proposes anti-money laundering (AML) and countering the financing of terrorism (CFT) obligations for PPSIs, and proposes specific obligations required by the GENIUS Act for PPSIs. The NPRM implements the GENIUS Act's directive to require PPSIs to maintain effective sanctions compliance programs.

IMPACT TO CREDIT UNIONS:

The NPRM treats PPSIs as "financial institutions" under the BSA, and in turn requires PPSIs to comply with suspicious activity reports (SAR), customer due diligence (CDD), sanctions, and other related BSA obligations. Such obligations for PPSIs could result in National Credit Union Administration (NCUA) examiners developing new supervisory expectations for credit unions that choose to engage in stablecoin related activities, requiring enhanced third-party risk management for credit union parents of PPSIs, assurance that SAR confidentiality is upheld between credit unions and their PPSI subsidiaries, and clearer contractual allocation of AML/CFT responsibilities between credit unions and PPSI subsidiaries. The NPRM strengthens parity between credit unions and PPSIs by requiring PPSIs to comply with a number of BSA obligations that already apply to credit unions.

KEY POINTS:

- PPSIs must operate AML/CFT programs, similar to those required by financial institutions under the BSA, that include AML policies and internal controls, independent testing and audits, employee training, a designated compliance officer, and risk assessments of stablecoin activity.
- PPSIs must monitor transactions for suspicious activity, file SARs with FinCEN as required, and not disclose SARs, or the existence of a SAR.

- PPSIs must uphold a sanctions compliance program to ensure that stablecoins are not used to transact with sanctioned countries or people by implementing strong internal controls for primary and secondary market stablecoin activity.

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: May 26, 2026 — **Submit here**.
- Comments due to Treasury: June 9, 2026
- Questions? Contact Jeremy Greenberg, Regulatory Advocacy Counsel, Innovation & Technology, America's Credit Unions
- Agency contacts: The FinCEN Regulatory Support Section, www.fincen.gov/contact and Assistant Director for Regulatory Affairs, OFAC, 202-622-4855, https://ofac.teasury.gov/contact-ofac.

QUESTIONS TO CONSIDER:

1. Where PPSIs are subsidiaries of credit unions, do any of these proposals for PPSIs present operational or legal challenges such that implementation would be overly burdensome or practically impossible? If so, which proposals and why?
2. Is the NPRM's description of an effective AML/CFT program sufficiently clear or is there anything further that FinCEN should consider adding in the final rule to clarify program effectiveness?
3. Are there particular types of payment stablecoin transactions or activities for which additional clarification regarding SAR reporting obligations would be beneficial? If so, which ones?

BACKGROUND:

The GENIUS Act, enacted on July 18, 2025, provides a comprehensive framework for the regulation of payment stablecoins. The GENIUS Act requires that a PPSI is treated as a financial institution for purposes of the BSA, and as such, subject to all Federal laws applicable to a financial institution relating to economic sanctions, money laundering (ML), and CDD. The GENIUS Act directs the Secretary of the Treasury to issue regulations, tailored to the size and complexity of the PPSI, implementing this provision of the GENIUS Act.

The GENIUS Act specifies that a PPSI's obligations include:

i. Maintenance of an effective AML program, which includes appropriate risk assessments and designation of an officer to supervise the program;
ii. Retention of appropriate records;
iii. Monitoring and reporting any suspicious transaction relevant to a possible violation of law or regulation;
iv. Maintenance of technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State law, rules, or regulations; and
v. Maintenance of an effective customer identification program, including identifying and verifying the PPSI's account holders, high-value transactions, and appropriate enhanced due diligence.

The GENIUS Act contains other provisions that control illicit risk in the payment stablecoin ecosystem. One of these provisions is the requirement that PPSIs only issue payment stablecoins if the issuer has the technological capability to comply and will comply with the terms of any "lawful order," which the GENIUS Act defines, in part, as an order issued or promulgated by a Federal agency or court to seize, freeze, burn, or prevent the transfer of payment stablecoins.

Regarding sanctions, the GENIUS Act expressly subjects PPSIs to all Federal laws applicable to a financial institution located in the United States relating to economic sanctions and requires PPSIs to maintain an effective economic sanctions compliance program, including verification of sanctions lists, consistent with Federal law.

SECTION-BY-SECTION ANALYSIS

Definitions

I. Amendment to 31 CFR 1010.100(T) – Financial Institution

- Amended to include "permitted payment stablecoin issuer."

II. Amendment to 31 CFR 1010.100(FF) – Money Services Business

- Amended to add PPSIs to the list of financial institutions that the term "money services business" shall not include.

III. Amendment to 31 CFR 1010.100(BBB) – Transaction

- Amended to add the issuance or redemption of a payment stablecoin as a type of transaction.

IV. Amendment to 31 CFR 1010.100(EEE) – Transmittal Order

- Amended to add a payment stablecoin as a subject of an order.

V. 31 CFR 1010.100(PPP) – Digital Asset

- Adopts GENIUS Act definition in 12 U.S.C. 5901(6).
- "Digital asset" means any digital representation of value that is recorded on a cryptographically secured distributed ledger.
    - "Digital asset" is limited to obligations to be imposed on PPSIs.

VI. 31 CFR 1010.100(QQQ) – Distributed Ledger

- Adopts GENIUS Act definition in 12 U.S.C. 5901(8).
- "Distributed ledger" means a technology in which data is shared across a network that creates a public digital ledger of verified transactions or information among network participants and cryptography is used to link the data to maintain the integrity of the public ledger and execute other functions.

VII. 31 CFR 1010.100(RRR) – Lawful Order

- Adopts GENIUS Act definition in 12 U.S.C. 5901(16), with modifications in light of a preexisting FinCEN regulatory definition.
- "Lawful order" means any final and valid writ, process, order, rule, decree, command, or other requirement issued or promulgated under Federal law, issued by a court of competent jurisdiction, or by an authorized Federal agency pursuant to its statutory authority that:
    1. Requires an individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated, to seize, freeze, burn, or prevent the transfer of payment stablecoins that the individual entity issued;
    2. Specifies the payment stablecoins or accounts subject to blocking with reasonable particularity; and
    3. Is subject to judicial or administrative review or appeal as provided by law.

VIII. 31 CFR 1010.100(SSS) – Payment Stablecoin

- Adopts GENIUS Act definition in 12 U.S.C. 5901(22), with modifications in light of preexisting FinCEN regulatory definitions and technical changes.
- "Payment stablecoin" means a digital asset:
    i. That is or is designed to be, used as a means of payment or settlement; and
    ii. The issuer of which:
        A. Is obligated to convert, redeem, or repurchase for a fixed amount of monetary value, but not for a digital asset denominated in a fixed amount of monetary value; and

B. Represents that such issuer will maintain, or create the reasonable expectation that it will maintain, the digital asset at a stable value relative to the value of a fixed amount of monetary value.

- "Monetary value" means a national currency or deposit (as defined by § 3 of the Federal Deposit Insurance Act (FDIC Act) (12 U.S.C. 1813)) denominated in a national currency.

- A "payment stablecoin" does not include a digital asset that is:

i. A national currency:

A. A Federal Reserve note (as the term is used in the first undesignated paragraph of § 16 of the FDIC Act (12 U.S.C. 411); or

B. A medium of exchange currently authorized or adopted by a domestic or foreign government including a monetary unit of account established by an intergovernmental organization or by agreement between two or more countries that is:

1. Standing to the credit of an account with a Federal Reserve Bank;
2. Issued by a foreign central bank; or
3. Issued by an intergovernmental organization pursuant to an agreement by two or more governments.

ii. A deposit (as defined in § 3 of the FDIC Act (12 U.S.C. 1813)) including a deposit recorded using distributed ledger technology; or

iii. A security, as defined in § 2 of the Securities Act of 1933 (15 U.S.C. 77b), § 3 of the Securities Exchange Act of 1934 (15 U.S.C. 78c), or § 2 of the Investment Company Act of 1940 (15 U.S.C. 80a-2). This definition applies and not the preexisting regulatory definition of "security" at 31 CFR 1010.100(ss).

IX. 31 CFR 1010.100(TTT) – Permitted Payment Stablecoin Issuer

- Modifies GENIUS Act definition in 12 U.S.C. 5901(23) to align with preexisting FinCEN regulatory definitions.
- "Permitted payment stablecoin issuer" means any individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated formed in the U.S. that is:

1.(A) A subsidiary of an insured depository institution that has been approved to issue payment stablecoins by a primary Federal payment stablecoin regulator; or

1.(B) a subsidiary of an insured credit union that has been approved to issue payment stablecoins by a primary Federal payment stablecoin regulator;

2. A Federal qualified payment stablecoin issuer; or

3. A State qualified payment stablecoin issuer.

- The insured depository institution definition modifies statutory paragraph A. by replacing the term with the GENIUS Act definition in 12 U.S.C. 5901(15), which includes two subparagraphs, one applying to insured depository institutions as defined in § 3 of the FDIC Act and a second for insured credit unions.

X. 31 CFR 1010.100(UUU) – Primary Federal Payment Stablecoin Regulator

- Modifies GENIUS Act definition in 12 U.S.C. 5901(25).
- "Primary Federal payment stablecoin regulator" means:
    1. For a subsidy of an insured depository institution, the appropriate Federal banking agency of such insured depository institution.
    2. For a subsidiary of an insured credit union, the NCUA.
    3. For a State chartered depository institution not covered in subparagraph (1), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), or the Board of Governors of the Federal Reserve System (Board); or
    4. For a Federal qualified payment stablecoin issuer, the OCC.

XI. 31 CFR 1010.100(VVV) – Federal Qualified Payment Stablecoin Issuer

- Modifies GENIUS Act definition in 12 U.S.C. 5901(25).
- "Primary Federal payment stablecoin issuer" means an entity that is approved by the OCC under 12 U.S.C. 5903 to issue payment stablecoins and is either:
    1. A nonbank entity;
    2. An uninsured national bank; or
    3. A Federal branch.

XII. 31 CFR 10110(WWW) – State Payment Stablecoin Regulator

- Modifies GENIUS Act definition in 12 U.S.C. 5901(30) to align with preexisting FinCEN definitions.
- "State payment stablecoin regulator" means a state agency that has the primary regulatory and supervisory authority in such state over entities that issue payment stablecoins.

XIII. 31 CFR 1010.100(XXX) – State Qualified Payment Stablecoin Issuer

- Adopts GENIUS Act definition in, 12 U.S.C. 5901(31) with modifications to align with preexisting FinCEN definitions.
- "State qualified payment stablecoin issuer" means an entity that is:
    1. Legally established under the laws of a State or Territory and Insular Possession and approved to issue payment stablecoins by a State payment stablecoin regulator; and
    2. Not an uninsured national bank chartered by the OCC pursuant to title LXII of the Revised Statutes, a Federal branch, or uninsured depository institution.

Proposed Amendment to 31 CFR 1010.810 – Delegation of Examination Authority

- Examination authority over PPSIs is delegated to federal agencies responsible for examining the same entities for safety and soundness and, where no such federal agency exists, to the IRS.

I. State Qualified Payment Stablecoin Issuers

- FinCEN delegates its examination authority to the IRS for PPSIs not examined by the OCC, Board, FDIC, and NCUA for safety and soundness.

II. Proposed 31 CFR 1010.810(b)(8) – Federal Qualified Payment Stablecoin Issuers

- A new paragraph is added to § 1010.810(b) to delegate examination authority to the primary Federal payment stablecoin regulators responsible for assessing a PPSI's safety and soundness.

Proposed Amendment to 31 CFR 1033.210 – AML/CFT Program Requirements for PPSIs

- AML/CFT obligations are imposed on PPSIs consistent with the program being proposed for the 11 types of financial institutions covered by BSA program requirements, with some modifications due to provisions of the GENIUS Act.

I. AML/CTF Program Overview

- Requirements are specifically defined for a PPSI to establish and maintain an effective AML/CFT program.
- This section adopts into regulation the AML Act's requirements that AML/CFT programs should be risk-based, applying such requirements to PPSIs to direct more attention and resources toward higher-risk customers and activities, consistent with the risk profile of the PPSI, rather than toward lower-risk customers and activities.
- Under § 1033.210 PPSIs are required to have an effective AML/CFT program and comply with the requirements of 31 U.S.C. 5318(h)(1) and § 1033.210 if the PSI:
    1. Establishes an AML/CFT program in accordance with paragraph (b) of § 1033.210; and
    2. Maintains an AML/CFT program by implementing the AML/CFT program in accordance with paragraph (c) of § 1033.210.
- PPSIs are required to conduct ongoing customer due diligence.
- AML/CTF Program Requirements
    - PPSIs must establish an AML/CFT program and then maintain the AML/CFT program by implementing the established AML/CFT program.
    - An AML/CFT program is "effective" and complies with the requirements of 31 U.S.C. 5381(h)(1) so long as it is established and maintained in accordance with applicable requirements.

- PPSIs must establish a risk-based set of internal policies, procedures, and controls that are reasonably designed to ensure compliance with the BSA and 31 CFR chapter X. Such policies, procedures, and controls must be reasonably designed to:
    1. The PPSI must identify, evaluate, and record its exposure to money laundering and terrorist financing risks by using risk assessment procedures that analyze its business operations, review and, when necessary, incorporate AML/CFT Priorities, and promptly update these assessments whenever the PPSI becomes aware of significant changes to its ML/terrorist financing (TF) risk profile.
    2. The PPSI must address and reduce its money laundering and terrorist financing risks in line with its risk assessment processes.
    3. The PPSI must continually perform customer due diligence.
- As part of an effective AML/CFT program, PPSIs are required to update their risk-based internal policies, procedures, and controlsas the PPSI's risk profile changes. The PPSI is also required to keep the employee training program and initiation of an independent testing mechanism current.
- PPSIs are required to establish an ongoing employee training program and independent AML/CFT program testing as part of its AML/CFT program.
- PPSIs are required to designate an individual responsible for establishing and implementing the AML/CFT program and coordinating and monitoring day-to-day compliance.
    - The individual is required to be located in the US and accessible to, and subject to oversight and supervision by, FinCEN and its designee, including the appropriate primary Federal payment stablecoin regulator.
- Minor deficiencies of an AML/CFT program would not necessarily mean that a PPSI has failed to implement the program.

II. Proposed 31 CFR 1033.210(b) – Program Establishment

- AML/CFT program requirements for PPSIs must have certain minimum elements comprised of:
    1. Internal policies, procedures, and controls;
    2. An independent audit function to test programs;
    3. A designated compliance officer; and
    4. An ongoing employee training program.

A. Proposed 31 CFR 1033.210(b)(1) – Internal Policies, Procedures, and Controls

- A PPSI's risk-based set of internal policies, procedures, and controls must be reasonably designed to:
    1. Identify, assess, and document ML/TF risks through risk assessment processes;
    2. Mitigate ML/TF risks consistent with the risk assessment processes, including by allocating more attention and resources toward higher-risk

customers and activities rather than toward lower-risk customers and activities; and

3. Conduct ongoing CDD.

- The level of sophistication of the internal policies, procedures, and controls should be commensurate with the size, structure, and complexity of the PPSI.

1. 31 CFR 1033.210(b)(1)(I) – Risk Assessment Processes

- The PPSI must establish and maintain risk assessment processes to:
  1. Evaluate the ML/TF risks of the PPSI's business activities, including products, services, distribution channels, customers, and geographic locations.
  2. Review and, as appropriate, incorporate the AML/CFT Priorities.
  3. Be updated promptly upon any change that the PPSI knows or has reason to know significantly changes the PPSI's ML/TF risks.

I. 31 CFR 1033.210(b)(1)(I)(A) – ML/TF Risks

- PPSIs are required to have risk assessment processes to evaluate the ML/TF risks of its business activities, including products, services, distribution channels, customers, and geographic locations.
  - Distribution channels refer to the methods and tools through which a PPSI opens accounts and provides products or services (including payment stablecoins).
- PPSIs may use a variety of sources to inform their risk assessment processes. Such sources may include:
  - Information obtained from other financial institutions;
  - Information generated from another source, such as that acquired from blockchain analytics (e.g., internet protocol (IP) addresses or device logins and related geolocation information);
  - Feedback from FinCEN, law enforcement, and financial regulators; and
  - Information identified from responding to § 314(a) requests (requiring financial institutions to search their records for transactions or accounts involving persons or entities suspected of ML/TF).
- Regardless of the source, PPSIs should take measures in their risk assessment processes to ensure this information is reasonably current, complete, and accurate.

II. 31 CFR 1033.210(b)(1)(I)(B) – AML/CFT Priorities

- PPSIs are required to review and incorporate the AML/CFT Priorities (as appropriate), which set out the priorities for the US government's AML/CFT policy as required by the AML Act and are designed to ensure that PPSIs' AML/CFT programs are aligned with those priorities.
    - PPSIs may use their judgment and their reasonable, risk-based determination whether to focus on a specific aspect of an AML/CFT Priority, rather than addressing all aspects of an AML/CFT Priority that may either may not be applicable or pose lower risks to the PPSIs.

III. 31 CFR 1033.210(b)(1)(I)(C) – Update Risk Assessment Processes

- PPSIs are required to update their risk assessment processes promptly upon any change that the PPSI knows or has reason to know significant changes its ML/TF risk profile.
- PPSIs may need to update its risk assessment process based on factors external to its operations that it knows or had reason to know significantly changes its ML/TF risk profile.

2. 31 CFR 1033.210(b)(1)(II) – Mitigate ML/TF Risks

- Examiners are expected to assess whether:

  1. A PPSI's resource allocation decisions are informed by, and consistent with, reasonably designed risk assessment processes; and
  2. With respect to implementation, whether the PPSI knows or should know of resource-related issues involving its internal policies, procedures, and controls and other mandatory elements that may result in the PPSI failing to implement its AML/CFT program in all material respects and failing to address such issues.

3. 31 CFR 1033.210(b)(1)(III) – Conduct Ongoing Customer Due Diligence

- PPSIs may need to consider (among other factors) established components of existing BSA programs including:
    - The type of entity seeking to establish a customer;
    - The jurisdiction in which they are domiciled;
    - The AML/CFT obligations they are subject to;
    - The customer's operating history;
    - The services the customer offers to its users;
    - The markets that the customer serves; and
    - The agents or intermediaries through which the customer may provide their services.

- PPSIs may need to consider information tailored to the stablecoin market including both information available from public blockchains and relevant off-chain considerations.

B. 31 CFR 1033.210(b)(2) – Independent Testing

- This evaluation typically includes a conclusion about the PPSI's overall compliance with AML/CFT statutory and regulatory requirements and sufficient information for the reviewer to reach a conclusion about whether the risk-based set of internal policies, procedures, and controls are reasonably designed and resources are well-allocated consistent with the PPSI's risk assessment process.
- PPSIs that do not employ outside auditors or consultants or lack internal audit departments may comply with this requirement by using internal staff who are not involved in the function being tested.
    - For these PPSIs, and PPSIs with other types of independent test arrangements, the AML/CFT officer, or any party who directly (and in some cases, indirectly) reports to the AML/CFT officer or equivalent, would generally not be considered sufficiently independent.
- For PPSIs that engage outside auditors or consultants, these PPSIs are required to ensure that the parties conducting the testing are not involved in functions related to the AML/CFT program at PPSIs.
- For testing, outside parties would not include government agencies, entities, or instrumentalities, such as a PPSI's primary Federal payment stablecoin regulator or State payment stablecoin regulator.
- PPSIs with less complex operations and lower risk profiles may consider a shared resource as part of a collaborative arrangement to conduct testing (as long as the testing is independent).

C. 31 CFR 1033.210(b)(3) – Designate an AML/CFT Officer

1. 31 CFR 1033.210(b)(3)(III) – Duties of the AML/CFT Officer

- PPSIs are required to designate an AML/CTF officer responsible for implementing the AML/CTF program and coordinating and monitoring day-to-day compliance with the requirements/prohibitions of the BSA and FinCEN's implementing regulations.
- The AML/CFT officer's access to resources may include:
    - Adequate compliance funds and staffing with the skills and expertise appropriate to the PPSI's risk profile, size, and complexity;
    - An organizational structure that supports compliance and effectiveness; and

    - Sufficient technology and systems to support the timely identification, measurement, monitoring, reporting, and management of the PPSI's ML/TF risks.
- An AML/CFT officer with conflicting responsibilities that adversely impact the officer's ability to effectively coordinate and monitor compliance generally would not fulfill this requirement.

2. 31 CFR 1033.210(b)(3)(I) and (II) – The AML/CFT Officer Located in the United States and Accessible to Regulators
- A PPSI's AML/CFT officer must be located in the US and accessible to, and subject to oversight and supervision by FinCEN and its designee.
- Personnel located outside of the US are permitted to perform certain AML/CTF functions.

3. 31 CFR 1033.210(b)(3)(IV) – Restriction on Officers with Felony Convictions
- This restriction applies to officers that supervise a PPSI's AML/CTF program.

D. 31 CFR 1033.210(b)(4) – Ongoing Employee Training Program
- PPSIs are required to establish an ongoing employee training program that would generally cover PPSI internal policies, procedures, and controls, which should reflect the results of the PPSI's risk assessment processes, the latest AML/CFT regulatory requirements, and other relevant information.
- The frequency of when the training occurs, and the content of the training, depends on the PPSI's ML/TF risk profile and the roles and responsibilities of the persons receiving the training.

III. 31 CFR 1033.210(d) – Written AML/CFT Program and Approval
- A PPSI's AML/CTF program must be written and made available to FinCEN or its designee upon request, which can include the appropriate agency with examination authorities delegated by FinCEN.
- The written program must be approved by the PPSI's board of directors or an equivalent governing body within the PPSI, or appropriate senior management.
- The approval encompasses each of the components of the AML/CFT program.
- PPSIs have significant flexibility in its chosen approval method.

IV. 31 CFR 1033.210(e) – AML/CFT Program Certifications
- PPSIs are required to make available to FinCEN, or its designee, upon request all certifications submitted to the PPSI's primary Federal payment stablecoin regulator or

State payment stablecoin regulator certifying that the PPSI has implemented an AML/CFT program.

4. CFR 1033.221 – Supervision and Enforcement

- PPSIs' AML/CFT programs must be aligned with the AML Act's emphasis on effectiveness and risk-based supervision, which includes three elements:

  1. Defining key terms;

  2. Outlining when FinCEN or the primary Federal payment stablecoin regulators would take an enforcement or supervisory action regarding certain kinds of AML/CFT program violations; and

  3. Outlining when the primary Federal payment stablecoin regulators would consult with FinCEN on potential supervisory actions.

I. 31 CFR 1033.221(a) – Definitions

- "AML/CFT Enforcement Action" means any formal or informal action taken by FinCEN that seeks to penalize, remedy, prevent, or respond to noncompliance with past or ongoing violations of, or past or ongoing deficiencies related to, an AML/CFT requirement.
- "AML/CFT Requirement" means a requirement of the BSA.
- "Significant AML/CFT Supervisory Action" means any written communication or other formal supervisory determination issued by FinCEN or a primary Federal payment stablecoin regulator, when acting under supervisory authority delegated by FinCEN, that identifies one or more alleged deficiencies, weaknesses, violations of law, or unsafe or unsound practices or conditions relating to:
  - An AML/CFT requirement;
  - Communicates supervisory expectations regarding actions or remedial measures required to correct the issue; and
  - Contemplates significant or programmatic actions or remedial measures to be taken by the PPSI.
  - Expressly excluded by this definition: Examiner observations, suggestions, or other informal comments.

II. 31 CFR 1033.221(b) – Enforcement and Supervision Policy

- A PPSI that has properly established an AML/CFT program would not be subject to an AML/CFT enforcement action based on a violation of § 1033.210 unless there is a significant systemic failure to implement an effective AML/CFT program for failing to implement, in all material respects, a properly established AML/CFT program.

- This rule would not affect the factors that FinCEN applies in the disposition of a violation once FinCEN has determined that such violation involves either:
    1. A Failure to properly establish an AML/CFT program; or
    2. A significant or systemic failure to implement an AML/CFT program.

III. 31 CFR 1033.221(c) and (d) – FinCEN Consultation and Consideration

- Establishes a notice and consultation framework applicable when a primary Federal stablecoin regulator, acting under supervisory authority delegated by FinCEN, intends to initiate a significant AML/CFT supervisory action.
- Before issuing such an action, the primary Federal payment stablecoin regulator is required to provide the Director of FinCEN with an opportunity to review the action and consider any input offered by the Director, which may include any view as to the effectiveness of the PPSI's AML/CTF program.
- The primary Federal payment stablecoin provider is required to provide written notice of their intent to take the action to the Director at least 30 days in advance of the proposed action, unless a shorter period is necessary.
- The notice must be accompanied by the relevant AML/CFT information underlying the proposed action. This may include, but not limited to:
    - Relevant portions of the draft report enforcement action;
    - Relevant examination workpapers supporting the proposed action; and
    - Relevant AML/CFT information submitted by the PPSI to the primary Federal payment stablecoin regulator.
- The Director of FinCEN would consider factors in determining whether to take an enforcement action or significant supervisory action with respect to PPSIs, including:
    - The factors set forth in 31 U.S.C. 538(h)(2)(B) (which covers the factors the Secretary of the Treasury considers in supervising and examining compliance with AML programs), as applicable;
    - The extent, if any, to which the PPSI has advanced the AML/CFT Priorities by providing highly useful information to law enforcement or national security officials; and
    - Any other factor the Director deems appropriate.

5. Amendment to 31 CFR 1010.230 – Collection of Beneficial Ownership Information

- PPSIs are required to collect beneficial ownership information about legal entity customers.
- PPSIs are required to have procedures related to verifying the identity of beneficial owners that would contain the same elements as 31 CFR 1022.220(a)(2), the customer identification rule for banks.

6. 31 CFR 1033.240 – Additional Technical Capabilities, Policies, and Procedures for PPSIs

- PPSIs must have the technical capabilities, policies, and procedures to block, freeze, and reject requirements and lawful order requirements.
    - Both obligations apply to secondary market activity and may also apply where a PPSI is authorized by its primary Federal payment stablecoin regulator or State stablecoin regulator to engage in digital asset service provider activities.

I. 31 CFR 1033.240(a) – Obligations Related to Blocking, Freezing, and Rejecting Certain Transactions

- PPSIs must have the infrastructure necessary to block, freeze, and reject impermissible transactions, but would not require a PPSI to make an independent determination that a transaction violates federal or state law.
- PPSIs' technical capabilities, policies, and procedures should account for identifying and blocking or rejecting payment stablecoin-related transactions that would violate US sanctions, including to identify and block stablecoins that are issued to or redeemed by blocked persons.

II. 31 CFR 1033.240(b) – Obligations Related to Lawful Order Compliance and Technical Capabilities

- Clarifies GENIUS Act requirements that a PPSI "may issue payment stablecoins only if the issuer has the technological ability to comply, and will comply, with the terms of any lawful order" (12 U.S.C. 5901(16)). Such obligations are ongoing rather than only in existence at the time a stablecoin is issued.
- PPSIs are required to consider and comply with all terms contained in lawful orders and apply to any lawful order, including those that relate to primary or secondary market activity.

7. 31 CFR 1033.310—1033.315 – Reports of Transactions in Currency

- PPSIs are required to comply with a Currency Transaction Report (CTR) obligations, which applies to transactions in currency of more than $10,000 conducted during a single business day.
- PPSIs are prohibited from structuring transactions to avoid the reporting requirement.
- Non-bank financial institutions are exempt from filing reports with respect to transactions between the institution and a commercial bank. Where a PPSI is also a bank, this exemption, and not the other exemption applicable to banks, would control.

8. 31 CFR 1033.3120 – Reports of Suspicious Transactions

I. PPSI SAR Obligations with Regards to Secondary Market Activity

- A PPSI would be afforded protection from liability provided by the BSA for any secondary market SAR voluntarily filed reporting a possible violation of law or regulation in good faith.
- For the purposes of the SAR obligation, a transfer is not a "transaction" conducted or attempted by, at, or through a PPSI only due to an interaction with a smart contract.

II. 31 CFR 1033.320(a) – Reports by PPSIs of Suspicious Transactions

- A PPSI is permitted to voluntarily report any transaction the PPSI believes is relevant to the possible violation of any law or regulation that is not otherwise required to be reported.
- PPSIs are required to report suspicious activity that involves or aggregates at least $5,000 in funds or other assets.
- PPSIs are required to report a transaction if they know, suspect, or have reason to suspect that the transaction (or pattern of transactions of which the transaction is part) if the transaction:
    i. Involves funds derived from illegal activity or are intended or conducted to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
    ii. Is designed, whether through structuring or other means, to evade the requirements of the BSA;
    iii. Has no business or apparent lawful purpose, and the PPSI knows of no reasonable explanation for the transaction after examining the available facts; or
    iv. Is included in all SAR rules enacted after 2001.
- Where more than one financial institution with a separate suspicious activity reporting obligation is involved in the same transaction, only one report jointly filed on behalf of all involved financial institutions

would be required, provided that the joint report contains all relevant facts and that each institution maintains a copy of the report and any supporting documentation.

- Where a PPSI is a subsidiary of a parent insured depository institution and both institutions are required to file a SAR, the parent will be permitted to file SARs on behalf of its PPSI subsidiary (and vice versa).

III. 31 CFR 1033.320(b) – Filing and Notification Procedures

- If a PPSI identifies a suspect, within 30 days of initial detection by the reporting PPSI, facts that may constitute a basis for filing a SAR, the PPSI would need to report the transaction by completing and filing a SAR with FinCEN in accordance with all form instructions.
- If a PPSI does not identify a suspect, a PPSI may delay filing for 30 days to identify a suspect.
- PPSIs need to collect and maintain supporting documentation for each SAR.
- For situations requiring immediate attention, such as suspected terrorist financing or ongoing money laundering schemes, PPSIs are required to notify immediately by telephone the appropriate law enforcement authority in addition o filing a timely SAR.
- PPSIs looking to voluntarily report suspicious transactions that may relate to terrorist activity may call FinCEN's Financial Institutions Hotline (1-866-556-3974) in addition to filing a timely SAR.
    - A PPSI may also, but not required to, contact its primary Federal payment stablecoin regulator to report such situations.

IV. 31 CFR 1033.320(c) – Retention of Records

- PPSIs must maintain copies of filed SARs and the underlying related documentation for a period of five years from the date of filing.
- Supporting documentation would need to be made available to FinCEN, any Federal, State, or local law enforcement agency, or any Federal regulatory authority that examines the PPSI for compliance with the BSA under the proposed rule, upon request of that agency or authority.

V. 31 CFR 1033.320(d) – Confidentiality of SARs

- A SAR and any information that would reveal the existence of a SAR are confidential and shall not be disclosed except as authorized in s§ 1033.320(d)(1)(ii).
- § 1033.320(d)(1)(i) generally provides that no PPSI, and no current or former director, officer, employee, or agent of any PPSI, shall disclose a SAR or any information that would reveal the existence of a SAR.
- Any PPSI and any current or former, director, officer, employee or agent of any PPSI that is subpoenaed or otherwise requests to disclose a SAR or any information that would reveal the existence of a SAR, must decline to produce the SAR or such information and are required to notify FinCEN of such request and any response.
- PPSIs are prohibited from disclosing voluntary reports of suspicious activity.
- The rules of construction that clarify the scope of the prohibition against the disclosure of a SAR by a PPSI remain qualified by, and subordinate to, the statutory mandate that revealing to one or more subjects of a SAR of the SAR's existence is a crime.
- Disclosure of SAR information by government authorities that have access to SARs other than in fulfillment of their official duties consistent with the BSA is prohibited.

VI. 31 CFR 1033.320(e) – Limitation of Liability

- Provides protection from liability (aka a safe harbor) for PPSIs making either required or voluntary reports of suspicious transaction, or for failures to provide notice of such disclosure to any person identified in the disclosure to the full extent provided by 31 U.S.C. 5318(g)(3).
- The protection extends to a PPSI and any current or former director, officer, employee, or agent of a PPSI.

VII. 31 CFR 1033.320(f) – Compliance

- FinCEN and its delegates will examine PPSIs' compliance with their obligation to report suspicious transactions.
- A PPSI's failure to comply with FinCEN's SAR filing requirements may constitute a violation of the BSA and FinCEN's regulations.

VIII. 31 CFR 1033.320(g) – Clarification Regarding Transactions

- Explicitly scopes out secondary market transfers from a PPSI's SAR reporting obligation.
- FinCEN preliminarily believes that attempting to further outline the definition of "transaction" by "scoping in" specific stablecoin related activities adds unnecessary complexity and could lead to the PPSI SAR obligation being overly or underly inclusive.

9. 31 CFR 1033.400 and 1033.410 – Recordkeeping Requirements for PPSIs

I. Application of Recordkeeping Obligations in §§ 1010(a)-(d)

- PPSIs must create and retain certain records for extensions of credit access of $10,000 and certain records of cross-border transfers of currency, monetary instruments, funds, checks, investment securities, and credit worth more than $10,000.
- PPSIs must maintain records related to any order issued under § 1010.370(a) for up to five years.

II. Application of Recordkeeping Obligations in §§ 1010(e) and (f)

- PPSIs are required to comply with the Recordkeeping Rule (§1010(e)), which requires financial institutions to collect and retain records for funds transfers and transmittals of funds in amounts of $3,000 or more.
- PPSIs are required to comply with the Travel Rule (§ 1010(f)), which requires financial institutions to transmit information on certain funds transfers and transmittals of funds to other financial institutions participating in the transfer or transmittal.

A. Amendment to 31 CFR 1010.100(eee) – Definition of Transmittal Order

- "Transmittal order" means an order that causes another financial institution to pay a fixed amount of money.
- This definition is amended to explicitly include payment stablecoins in addition to money.

B. Amendment to 31 CFR 1010.410(e)(6) – Scope of Recordkeeping Obligation

- The recordkeeping requirements of the Recordkeeping Rule would not apply to the transmittals of funds in which both the transmitter and the recipient are either a PPSI bank, broker-dealer, futures commission merchant, introducing broker in commodities, or mutual fund.

10. 31 CFR 1033.520 and 1033.540 – Special Information-Sharing Procedures

- FinCEN proposes applying the information-sharing provisions of current §§ 1010.520 and 1010.540 to PPSIs. As a result, PPSIs must implement §§ 314(a) and 314(b) of the USA PATRIOT Act (which mandate information sharing with Federal law enforcement and allows voluntary sharing between financial institutions, respectively).
    - § 1033.520 requires financial institutions to search their records upon receipt of a request from FinCEN and provide information in return.
    - § 1033.540 applies to financial institutions that are required to have AML/CFT programs, or are treated as having satisfied that requirement, and is a voluntary information sharing tool of which a financial institution may, but is not required to, avail itself.

11. 31 CFR 1033.600—1033.630 – Special Standards of Diligence; Prohibitions, and Special Measures

- Most of the provisions in part 1010 subpart F are applied to PPSIs, including enhanced due diligence (EDD) for correspondent and private banking accounts and some other special features.
- § 1033.600 states generally that PPSIs are subject to the special standards of diligence, prohibitions, and special measures of part 1010 subpart F.

I. Definition of "Correspondent Account" and "Covered Financial Institution"

- The definition of "account" in § 1010.605(c) as applied to the meaning of a correspondent account is amended to include accounts with PPSIs.
- The definition of "correspondent account" is amended so that PPSIs are required to implement obligations related to the BSA's explicit references to enhanced due diligence.
- The definition of "covered financial institution" is amended to include PPSIs, which results in PPSIs being subject to provisions implementing special standards of due diligence for correspondent accounts established or maintained for foreign financial institutions and private banking accounts established or maintained for non-U.S. persons.

II. Special Standards for Diligence

- PPSIs are required to meet special standards of due diligence for correspondent accounts for foreign financial institutions and banks and for private banking accounts that include policies, procedures, and

controls that are reasonably designed to detect and report any known or suspected ML or suspicious activity conducted through or involving any such correspondent or private banking accounts.

III. Special Measures

- By incorporating PPSIs into the definition of "covered financial institutions" special measures are imposed on PPSIs with respect to interactions with identified foreign entities.

Application of Sanctions Program Requirement

- Stablecoin issuers that qualify as PPSIs are required to comply with US sanctions under existing Federal law. Meaning they must generally:
  - Block the property and interests in the property of blocked persons;
  - Reject prohibited transactions involving certain persons, jurisdictions, or activities; and
  - Retain certain records and file reports with OFAC.

A. Recordkeeping and Reporting

- PPSIs must comply with standard recordkeeping and reporting requirements as found in 31 CFR part 501.
- PPSIs must provide to OFAC upon request any and all certifications submitted to the PPSI's Federal payment stablecoin regulator or State payment stablecoin regulator certifying that the PPSI has implemented an effective sanctions compliance program.

B. Effective Sanctions Compliance Program

- PPSIs must adopt a sanctions compliance program including the five key elements in line with OFAC's 2019 Compliance Framework (at a minimum):
  1. Senior management and organizational commitment;
  2. Risk assessment;
  3. Internal controls;
  4. Testing and auditing; and
  5. Training.

1. 31 CFR 502.201 (b)(1) – Senior Management and Organizational Commitment

- PPSIs' senior management are required to review and approve a PPSI's sanctions compliance program and support the sanctions compliance program's effective implementation, including by ensuring the sanctions compliance program, at a minimum:

i. Applies to all payment stablecoin-related activity;
ii. Has sufficient resources, including necessary investments in human capital, expertise, and information technology to carry out the requirement that PPSIs conduct risk assessments, maintain internal controls, conduct testing and auditing, and maintain a risk-based sanctions compliance training program;
iii. Is fully integrated into the PPSI's ongoing stablecoin-related operations;
iv. routinely provides risk updates, including test results, to senior management and other appropriate personnel within the PPSI; and
v. provides sufficient authority and autonomy to the compliance function to manage effectively U.S. sanctions risk for the entire PPSI.

- A PPSI's senior management includes individuals responsible for monitoring performance across the organization, including its sanctions compliance program.
    - As applicable this could include supervisory, managerial, and executive employees, and can include its board of directors, owners, operators, and other leadership personnel depending on the PPSI's governance structure.
    - The composition of a PPSI's senior management is a fact-specific matter depending on each individual PPSI with PPSIs having the flexibility in determining which members of senior management ensure an effective sanctions compliance program.
- A PPSI' senior management is required to support the sanctions compliance program's effective implementation by ensuring the program includes, at a minimum, certain key components:
    - The sanctions compliance program applies to all payment stablecoin-related activity;
    - The sanctions compliance program has adequate resources tailored to a PPSI's particular circumstances;
    - The sanctions compliance program is fully integrated into a PPSI's ongoing stablecoin-related operations;
    - Senior management, and other appropriate personnel, routinely receive risk updates, including test results, from the sanctions compliance program; and
    - The sanctions compliance program has sufficient authority and autonomy to function and conduct timely and effective operations.

2. 31 CFR 502.201 (b)(2) – Risk Assessments

- PPSIs must conduct sanctions-related risk assessments by:
    i. Using the risk assessments to inform the PPSI's operation of its sanctions compliance program, including revising internal controls and training as appropriate;

ii. Using the risk assessments to inform the PPSI's operation of its sanctions compliance program;
iii. Revising risk assessments as appropriate to account for any identified US sanctions violations or deficiencies, new products, services, mergers, or acquisitions, and any other factors that may affect a PPSI's risk profile.

3. 31 CFR 502.201 (b)(3) – Internal Controls
    - PPSIs are required to establish and maintain a system of risk-based internal controls—including technical capabilities and written policies and procedures—applicable to all payment stablecoin-related activity.
        - This is required whether this activity occurs on the primary or secondary market, that identifies, blocks, and/or rejects transactions that may violate or would violate US sanctions and retains relevant records in accordance with OFAC regulations.
    - PPSIs should implement risk-based sanctions controls on transactions, including the secondary market, to satisfy this requirement.
    - OFAC's Virtual Currency Industry Guidance provides examples of best practices for internal controls, including with respect to transaction monitoring and sanctions screening, for digital assets participants, which will likely be relevant for PPSIs.
    - Technical internal controls should enable the PPSI to clearly and effectively identify, interdict, escalate, and report activity that may be prohibited by the regulations and laws administered by OFAC.
    - PPSIs should generate and maintain records pertaining to activity that may be prohibited by OFAC as part of their internal controls regime.
    - PPSIs must continually update their technical internal controls (including risk-based sanctions screening), which ensure the internal controls effectively address amended or updated US sanctions authorities and applicable US sanctions risks.
        - Internal controls should be capable of adjusting rapidly to new OFAC designations, prohibitions, requirements, and guidance, and of effectively identifying risk exposure that may warrant heightened due diligence.
        - Relevant guidance may include risks identified in advisories, alerts, or notices issued by Treasury or other relevant US government agencies.
            - PPSIs should consider using such information, along with other open source and proprietary information, to conduct proactive diligence to identify and mitigate potential sanctions risks.

- Risk-based internal controls established by the PPSI must be documented in writing and clearly communicated to all relevant personnel and stakeholders.
    - Such internal control documents must be routinely reviewed and revised such that there is timely and appropriate action to remediate any identified compliance gaps or deficiencies.
    - The process of routinely reviewing and revising written policies and procedures should incorporate frequent testing of technical internal controls to ensure effectiveness and sufficiency.
    - If and when a PPSI identifies a weakness in its internal controls system, the PPSI should take immediate and effective action, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.
- PPSIs may consider using a variety of tools to develop and implement internal controls, including external resources, rather than uniform "one-size-fits-all" internal control system requirements.

4. 31 CFR 502.201 (b)(4) – Testing and Auditing
- PPSIs are required to establish and maintain an independent testing or audit function, accountable to senior management, with sufficient resources, expertise, and authority to identify US sanctions compliance-related weaknesses and deficiencies.
- PPSIs must ensure that qualified personnel routinely perform comprehensive, independent, and objective testing or auditing of the effectiveness of the sanctions compliance program and its functions.
- Such testing and auditing results are used to identify and implement any needed updates or enhancements to the sanctions compliance program, and PPSIs must maintain and provide to OFAC upon request records of any such testing and auditing results and enhancements.
- An independent testing or audit function can be either external or internal to a PPSI.
    - If internal, controls must be in place to ensure audits or testing are sufficiently independent. Criteria to assess independence can vary based on a variety of factors, including:
        - A PPSI's internal corporate structure;
        - The internal auditor's accountability to senior leadership and the board of directors; and
        - The training and expertise possessed by the internal auditor.
- Based on the 2019 Compliance Framework, a testing and auditing program should be tailored to address the sanctions risks accompanying the PPSI's operations, and results should be used to:

- Implement updates;
- Remediate compliance gaps; and
- Make PPSIs aware of how its products and services are performing against the sanctions compliance program's internal control benchmarks.

5. 31 CFR 502.201 (b)(5) – Training

- PPSIs must establish and maintain a risk-based compliance training program that is:
  i. Performed at least annually and with a frequency appropriate to the PPSI's risk assessments and risk profile;
  ii. Provided to all relevant personnel and stakeholders;
  iii. Appropriately tailored to each trainee's role and responsibilities;
  iv. Modified to reflect risk assessments findings and identified deficiencies in the sanctions compliance program, including testing and audit findings; and
  v. Designed to include easily accessible resources and materials for all relevant personnel and stakeholders.
- PPSIs have discretion in setting a training cadence that aligns with a PPSI's circumstances, provided a PPSI meets the minimum of an annual training.
- PPSIs must modify training programs to reflect any findings of risk assessments and identified deficiencies in their sanctions compliance program.

C. Effective Sanctions Compliance Program

- Payment stablecoin-related activity is defined as capturing the range of activities involving a PPSI's payment stablecoin, such as issuance, redemption, and custody, including activity on the secondary market.
- "Permitted payment stablecoin issuer" is defined as consistent with the term in the GENIUS Act, but with the modification in how "person" is defined to match the definition in OFAC's regulations: "individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated."

1. 31 CFR 502.301 – Knowingly

- "Knowingly" means with respect to conduct, a circumstance, or a result means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

2. 31 CFR 502.303 – Payment Stablecoin-Related Activity

- "Payment stablecoin-related activity" is defined as including issuing, trading, holding, transacting, transferring, redeeming, or any other activity involving a

payment stablecoin issued by a PPSI from the time of issuance until the payment stablecoin's removal from circulation, whether on the primary or secondary market, including through redemption or by any other means.

3. 31 CFR 502.304 – Permitted Payment Stablecoin Issuer; PPSI
   - "Permitted payment stablecoin issuer" is defined consistently with the definition provided in the GENIUS Act:
     - A person formed in the US that is—
       - A. A subsidiary of an insured depository institution that has been approved to issue payment stablecoins under § 5904 of the GENIUS Act;
       - B. A Federal qualified payment stablecoin issuer; or
       - C. A State qualified payment stablecoin issuer.
     - OFAC replaces the word "person" with "individual, partnership, company, corporation, association, trust, estate, cooperative organization, or other business entity, incorporated or unincorporated."

D. 31 CFR 502.401 and 502.402 – Penalties
- § 502.401(a) imposes civil monetary penalties of not more than $100,000 per day for PPSIs that materially violate the requirement to maintain an effective sanctions compliance program.
- § 502.401(b) provides an additional $100,000 penalty for each day during which a PPSI knowingly participates in a violation of the same.
- If a PPSI does not pay the penalty imposed by § 502.401, § 502.402 authorizes OFAC to refer the matter for administrative collection measures by Treasury or the Department of Justice (DOJ) for appropriate action to recover the penalty in a civil suit in a federal district court.

Final Rule Effective Dates

- Rules become effective 12 months after issuance of final rules.

Key Questions Presented by FinCEN and OFAC for Public Comment:

The NPRM presents in total over fifty discrete questions for comment. The following items are a subset of those questions, reflecting topics of key importance in terms of PPSIs' AML/CFT and sanctions compliance program requirements.

1. Are FinCEN's proposed definitions sufficiently clear? Should the definitions be expanded or narrowed in any respect?
2. In what respect should a PPSI's AML/CFT program account for risks on the secondary market?
3. Is FinCEN's proposed language specifying PPSIs must have the technical capabilities to block, freeze, and reject impermissible transactions occurring on the secondary market appropriately scoped and sufficiently clear? Does it capture activity it should not? Does it leave out activity it should include?
4. Is FinCEN's proposal clear regarding SAR obligations relating to secondary market activity. If not, why not and how can it be improved?
5. Is clarification needed on how the proposed SAR reporting requirements interact with PPSIs' obligations related to blocking, freezing, and rejecting transactions, recordkeeping, or responding to lawful orders?
6. To what extent is it clear how payment stablecoins should be treated for purposes of FinCEN's recordkeeping requirements, including whether payment stablecoins should be considered "money," "funds," "currency," or another category under the proposed rule?
7. Are there aspects of the special standard of diligence framework that would benefit from clarification or modification when applied to PPSIs?
8. Are there types of relationships, accounts, or arrangements involving PPSIs that may raise questions about whether they should be treated as correspondent accounts, private banking accounts, or neither?
9. FinCEN is proposing an effective date of 12 months from the date of issuance of the final rule to allow sufficient time for PPSIs to review and implement its requirements. Does this timeframe allow for sufficient time to review and implement requirements?
10. What best practices would PPSIs consider in developing and implementing policies, procedures, and internal controls designed to ensure ongoing compliance with the proposed effective sanctions compliance program requirements?