HOWELL JACKSON

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C16

Submitter Information

Name: Howell Jackson

Submitted Date: 08/21/2026

See attached pdf file.

HARVARD LAW SCHOOL

HOWELL E. JACKSON
James S. Reid, Jr., Professor of Law
Lewis 312
Cambridge, Massachusetts 02138
Tel. (617) 495-5466
hjackson@law.harvard.edu

August 21, 2026

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

Comment Letter on Proposed Rule: Permitted Payment Stablecoin Issuer Customer Identification Program (*Submitted in response to: Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37,235 (June 22, 2026), RIN 1557-AF53.*

To the Financial Crimes Enforcement Network, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration (the Agencies):

I am the James S. Reid, Jr., Professor of Law at Harvard Law School. My research interests focus on financial regulation. I have written numerous articles on the subject and am the coauthor of Jackson & Tahyar, Financial Regulation: Law and Policy (Foundation Press 4th ed 2025). I served as a senior advisor on digital asset policy for the National Economic Council from 2023 to 2024.

I appreciate the opportunity to comment on the joint notice of proposed ruleaking ("NPRM") concerning customer-identification-program ("CIP") requirements for permitted payment stablecoin issuers ("PPSIs"). For purposes of this letter, I accept the proposal's central judgment: at present, CIP duties are to be keyed to direct, account-like relationships between a PPSI and its customers, rather than extended to every person who subsequently acquires, holds, or receives a transfer of a payment stablecoin on a public blockchain.

My recommendations for revision are thus limited. I do not invite the Agencies to alter the text of the proposed regulations or to impose a universal CIP requirement for secondary-market activity at this time. Instead, I recommend the Agencies adopt several clarifications in the preamble to the final rule. Those clarifications can preserve the proposal's account-centered architecture while making clear that voluntary, well-governed experimentation with secondary-market controls is permissible and that CIP policies for PPSIs in the future may be refined to reflect improvements and innovations in the technologies for monitoring secondary market transactions in stablecoins.

This letter responds in particular to the NPRM's request for comment on whether and how the proposal might better accommodate innovation with respect to secondary-market activity. See 91 Fed. Reg. at 37,244. I recommend that the final preamble expressly state that:

- A PPSI remains free to adopt voluntary, risk-based identification, credentialing, monitoring, and transfer-control measures for secondary-market activity involving its stablecoin, including privacy-preserving "whitelist" or credential-based arrangements;
- The decision not to require such measures in this CIP rulemaking reflects present technological and operational constraints, not a conclusion that secondary-market activity is categorically beyond the appropriate concern of BSA regulation or future PPSI rulemaking; and
- Voluntary use of reasonable enhanced controls does not, without more, establish a broader CIP duty or expose an issuer to hindsight supervisory liability merely because an emerging control does not ultimately prevent every instance of illicit activity.

Those clarifications would preserve an administrable CIP rule today while encouraging the responsible private-sector experimentation that Treasury itself has identified as important to improving digital-asset AML/CFT controls.

I. The proposal plausibly centers CIP on issuer-customer accounts

The GENIUS Act supplies two related instructions. It treats a PPSI as a financial institution for purposes of the Bank Secrecy Act ("BSA") and directs that a PPSI maintain an effective CIP, including identification and verification of account holders with the PPSI. See 12 U.S.C. § 5903(a)(5). Read together, those provisions incorporate PPSIs into the BSA framework while directing the Agencies to adapt CIP requirements to the distinctive structure of payment-stablecoin activity.

The proposed rule represents a credible response to these instructions even if it does not go as far as some may prefer. The proposal defines the relevant account relationship in functional terms and distinguishes a primary-market relationship—such as direct issuance, redemption, custody, or another direct service relationship with the issuer—from secondary-market activity in which the PPSI is not a party, apart from the operation of a smart contract. See 91 Fed. Reg. at 37,236–38. That distinction is defensible at this time. It identifies the settings in which a PPSI ordinarily can obtain and verify customer information, assign compliance responsibility, and operate a CIP in a manner comparable to other BSA-regulated financial institutions.

The distinction also avoids treating possession of a transferable token, without more, as the equivalent of opening an account with its issuer. A person who obtains a stablecoin from another holder – whether through an exchange or through a decentralized protocol – may have no direct relationship with the issuer. By contrast, a person who later establishes a direct redemption, custody, or other account-like service relationship with the PPSI should be subject to the issuer's

CIP at the point at which that relationship is formed. The final rule will, I anticipate, retain this administrable boundary.

II. Illicit finance concerns remain substantial for secondary market transactions in stablecoins

The account-centered CIP approach should not, however, be understood to minimize the illicit-finance and sanctions risks that can arise after a payment stablecoin leaves the issuer's direct customer relationship. The NPRM itself recognizes the relevance of stablecoins to fraud, sanctions evasion, terrorist financing, narcotics trafficking, and other illicit activity, as well as the particular challenges posed by rapid settlement, pseudonymous addresses, self-hosted wallets, and smart-contract-based transfers. See 91 Fed. Reg. at 37,237–38.

The existing literature likewise explains why downstream circulation matters. Jiaying Jiang's recent article, Crypto Money Laundering, examines how money laundering operates in the crypto ecosystem and the difficulties of applying existing AML rules in decentralized settings. See Jiaying Jiang, Crypto Money Laundering, 41 Berkeley Tech. L.J. 199 (2026). Her earlier work also identifies the diversification of crypto-related illicit conduct—including sanctions evasion, mixers, shadow money-services businesses, ransomware, and decentralized stablecoins—and explains why technology-enabled regulatory collaboration is needed to respond effectively. See Jiaying Jiang, Technology-Enabled Co-Regulation as a New Regulatory Approach to Blockchain Implementation, 82 U. Pitt. L. Rev. 829, 839–40, 856–73 (2022).

Nor does the fact that a PPSI is not a named counterparty to a secondary-market transfer eliminate the policy importance of that transfer. Payment stablecoins are designed to circulate across wallets, platforms, and protocols. In many business models, a relatively small group of direct institutional customers may acquire or redeem tokens from the issuer, while economically significant circulation occurs later through intermediaries and secondary markets. The disparity between initial onboarding and downstream use is therefore a genuine AML/CFT challenge.

The Agencies' earlier joint proposed rule on PPSI AML/CFT and sanctions-compliance programs confirms that the GENIUS Act's implementation framework does not end with primary-market CIP. See Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, 91 Fed. Reg. 18,582 (Apr. 10, 2026) ("PPSI AML/CFT NPRM"). That proposal separately addresses the primary- and secondary-market distinction and recognizes the importance of issuer capabilities to block, freeze, reject, or otherwise address transactions involving stablecoins, including activity that occurs in the secondary market. See id. at 18,585–89. While the proposed CIP rule limits the specific account-opening obligation to direct relationships, the broader GENIUS Act and implementing framework nevertheless contemplate that PPSIs will maintain risk-based AML/CFT and sanctions programs that take account of relevant secondary-market risks and available issuer controls. Cf. 91 Fed.

Reg. at 37,239 n.57 (noting that the term "account" in the BSA can have different meanings in different contexts).

Treasury's March 2026 Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets ("Innovation Report") makes the point in a complementary way. The Report identifies the speed, cross-border character, and perceived anonymity of digital assets as features that can be exploited by illicit actors. It specifically describes stablecoins as an element of complex laundering processes involving bridging, swapping, mixers, and cash-out activity. See Treasury, Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets 5–9 (Mar. 2026) ("Innovation Report").

At the same time, the Agencies have determined in this proposal that a universal secondary-market CIP mandate is not yet operationally realistic. See 91 Fed. Reg. at 37,279 ("FinCEN and the Agencies assess that [secondary market application of] a CIP obligation would be nearly impossible for PPSIs to implement and could potentially cripple the industry.") No single PPSI can necessarily identify every downstream wallet holder or reliably distinguish all legitimate from illicit transactions across the diversity of wallets, exchanges, bridges, and DeFi protocols through which its token might circulate. A rule that imposed such a mandate before the underlying identity and interoperability infrastructure is mature could produce substantial cost, privacy, and compliance uncertainty without commensurate improvement in illicit-finance detection.

The Agencies' determination does not mean that secondary-market risk is irrelevant. Rather, the conclusion is based on an assessment that available technology, industry architecture, and operational capacities do not yet support a uniform mandatory CIP obligation that reaches all secondary-market activity. The final rule's preamble should say so clearly, while recognizing that technological innovations and an improved AML/CFT toolkit may in the future make it feasible and appropriate to impose greater secondary-market CIP responsibilities on PPSIs.

III. The final preamble should expressly preserve voluntary experimentation

Because PPSI experimentation could materially contribute to the development of these new technologies, the final rule's preamble should confirm that nothing in the rule prevents a PPSI from voluntarily adopting additional, risk-based safeguards for secondary-market activity involving its stablecoin. An explicit clarification along these lines would be useful even if the Agencies view it as implicit in the proposed rule.

Such a clarification would promote private innovation. A PPSI may have sound compliance or commercial reasons to offer a stablecoin that can circulate only, or preferentially, among wallets with specified identity credentials or other compliance attestations. Institutional users, regulated intermediaries, and firms with substantial reputational or legal exposure may value greater assurance concerning the provenance of tokens they receive or the compliance status of counterparties. In other words, there may well be a market for stablecoins with robust restrictions on secondary market transactions.

Voluntary arrangements of this sort would permit PPSIs to experiment with controls that better address secondary market trading risks without requiring the Agencies to impose one architecture on all issuers today.

Potential tools include the following:

- Reusable digital credentials issued after compliant identity verification;
- Privacy-preserving proofs, including zero-knowledge proofs, by which a wallet can demonstrate that its holder satisfies a specified identity, jurisdictional, sanctions-screening, or eligibility condition without publicly revealing unnecessary personal information;
- Trusted identity attestations or interoperable credential systems;
- Permissioned or credential-gated wallet frameworks;
- Smart-contract-based rules that permit, condition, pause, freeze, or restrict transfers in accordance with documented risk controls; and
- Blockchain analytics, APIs, and other monitoring tools that support a risk-based assessment of downstream activity.

Acknowledging the permissibility of PPSI experimentation with these tools should not be confused with a claim that all PPSIs must now police every downstream transfer. But acknowledging the permissibility of issuer-level experimentation has the potential to produce stablecoin products with enhanced compliance assurances while generating practical evidence about effectiveness, cost, privacy, interoperability, and supervisory treatment.

Treasury's Innovation Report strongly supports preserving that room for responsible experimentation. The Report identifies AI, digital identity, blockchain monitoring and analytics, and APIs as technologies that may improve the effectiveness of AML/CFT compliance while reducing friction for legitimate users. It endorses a technology-neutral, risk-based approach; identifies responsible innovation, stakeholder collaboration, and coordination of standards as central policy principles; and states that Treasury will use convening, guidance, and coordination with supervisors to support the use of innovative tools. See Innovation Report 11–12, 17–30.

Of particular relevance, the Report explains that digital-identity technologies can support verification and the reuse of credentials, while privacy-enhancing approaches may enable users to demonstrate selected attributes without exposing all underlying information. See Innovation Report 17–22. The final CIP rule need not prescribe a particular technical solution. It should, however, avoid any implication that a PPSI's voluntary use of such measures for secondary-market activity is suspect, prohibited, or an implicit admission that the measures are already required.

IV. Voluntary controls should not create hindsight liability

An explicit preambular clarification is particularly important because voluntary experimentation may otherwise be chilled by uncertainty about supervisory consequences. A PPSI that elects to adopt enhanced identity or transfer controls should not face the risk that its choice creates a legal duty to extend CIP to all secondary-market activity, or that the failure of a new control to detect every instance of illicit use establishes a CIP violation.

Accordingly, the preamble should state that a PPSI's adoption of supplementary, voluntary controls for secondary-market activity does not, standing alone:

- Expand the scope of accounts subject to the final CIP rule;
- Establish that persons reached by those controls are "account holders" for purposes of the rule;
- Constitute an admission that the controls are legally required; or
- Subject the PPSI to adverse supervisory treatment merely because a reasonable, good-faith pilot or control does not prove fully effective.

This is not a request for immunity from the BSA, sanctions requirements, or ordinary supervisory oversight. A PPSI that adopts a control should do so responsibly, document its governance and risk assessment, accurately represent the control's capabilities, and comply with other applicable law. Nor should a PPSI be permitted to use a voluntary program as a pretext for misleading customers, evading compliance obligations, or collecting information without appropriate privacy and cybersecurity safeguards.

The more modest—and important—point is that regulators should not penalize good-faith innovation merely because a PPSI elects to go beyond the regulatory minimum or because an early-stage technology has limitations. The Innovation Report itself calls for supervisors and examiners to assess innovative tools properly and fairly. See Innovation Report 11–12. The final rule can reinforce that policy by affirmatively welcoming carefully governed experimentation.

V. The final preamble should preserve a path for future reassessment

The final preamble should also make clear that its treatment of secondary-market activity is based on the current state of technology and market development. The Agencies need not now decide whether future tools will make broader customer-identification, credentialing, or transaction-control expectations appropriate for some or all PPSIs. Indeed, the development of interoperable digital identity, privacy-preserving credentials, wallet-level attestations, and more capable analytics may materially change the feasibility analysis over time.

A clear statement to this effect would have three benefits. First, it would accurately describe the limited nature of the present rulemaking: a decision not to impose a universal secondary-market

CIP duty now does not resolve the appropriate scope of future AML/CFT obligations. Second, it would give innovators a reason to invest in tools capable of addressing the distinctive challenges of public-blockchain circulation. Third, it would facilitate a productive feedback loop: voluntary pilots, supervisory engagement, and public-private collaboration can provide the Agencies with evidence that informs later guidance or rulemaking.

The Innovation Report expressly contemplates that Treasury will support responsible innovation, collaborate with stakeholders and supervisors, and coordinate technical principles and standards to facilitate the adoption of emerging AML/CFT technologies. See Innovation Report 11–12. The final CIP rule should be framed as an early, practical step in that evolution —not as a conclusion that secondary-market safeguards are permanently impracticable or beyond regulatory reach.

VI. Recommended Clarifications to the Preamble for the Final Rule

I respectfully recommend that the final rule's preamble include language substantially along the following lines:

- The final rule does not prohibit a PPSI from voluntarily establishing and operating a customer identification program, or related identification and verification controls, for secondary-market transactions involving its payment stablecoins. A PPSI may experiment with new technologies and operational arrangements designed to identify or verify persons participating in such transactions, including reusable or interoperable digital credentials, privacy-preserving verification methods, zero-knowledge proofs, trusted identity attestations, credential-based or permissioned wallet frameworks, and smart-contract-based controls. Nothing in this rule limits a PPSI's ability to employ such voluntary measures, provided that the PPSI otherwise complies with applicable law.

- A PPSI's good-faith decision to experiment with voluntary secondary-market CIP measures does not, by itself, establish that those measures are required by this rule or that persons reached by them are account holders for purposes of this rule. Nor should a PPSI be subject to adverse supervisory or enforcement consequences merely because a reasonable, well-governed pilot or emerging technological control does not prevent every instance of illicit activity. This clarification does not excuse a PPSI from compliance with applicable BSA, sanctions, consumer-protection, privacy, cybersecurity, or other legal requirements; rather, it is intended to ensure that the possibility of legal or supervisory hindsight does not deter responsible efforts to develop more effective secondary-market identification tools.

- The rule's account-centered treatment of secondary-market transactions reflects the Agencies' assessment of the technologies and operational capabilities presently available

> to PPSIs and the digital-asset market. It does not represent a determination that a more robust CIP framework for secondary-market activity would be impermissible or inappropriate as technology develops. The Agencies should reserve their authority to reconsider the treatment of secondary-market transactions in a future rulemaking in light of practical experience, improved identity and verification tools, and relevant risk information. That reconsideration may include more robust CIP obligations for secondary-market activity and, where supported by future technological developments and the statutory framework, revisions to the definition of a PPSI "account" for CIP purposes.

This suggested language would not alter the proposed rule's basic legal architecture. It would instead make explicit three propositions that should guide its implementation: the direct account relationship remains the present CIP trigger; secondary-market risk remains a serious policy concern, which is addressed only in part by the broader AML/CFT and sanctions framework; and voluntary, privacy-conscious innovation can promote competition and support the development of technologies that could allow for more robust and effective oversight of secondary market transactions in stablecoins.

* * * * *

For purposes of this letter, I accept the NPRM's account-centered approach to CIP obligations and do not now urge the Agencies to impose a universal requirement that PPSIs identify all secondary-market holders or counterparties at this time. As the Agencies note, such a requirement may not yet be demonstrably feasible or sufficiently mature to serve as a uniform regulatory baseline.

The final rule should nevertheless invite responsible progress on the oversight of secondary market transactions, including voluntary customer identification tools. By expressly reserving PPSIs' freedom to experiment with enhanced secondary-market controls, avoiding hindsight liability for good-faith pilots, and recognizing that today's feasibility judgment may change as technology develops, the Agencies can promote innovation without sacrificing clarity or enforceability. That approach is fully consistent with Treasury's stated commitment to technology-neutral, risk-based AML/CFT regulation, the existing PPSI AML/CFT and sanctions framework, and responsible public-private collaboration in the digital-asset sector.

Respectfully submitted,

Howell E. Jackson

James S. Reid, Jr., Professor of Law
Harvard University