

**Global Blockchain Business Council (GBBC) USA:
Response to FinCEN Request for Comment on Permitted
Payment Stablecoin Issuer Customer Identification Program
(Docket FINCEN-2026-0101)**

General Remarks:

GBBC appreciates the opportunity to provide feedback on the proposed customer identification program requirements for permitted payment stablecoin issuers (PPSIs). GBBC recommends a clear, risk-based, and technology-neutral framework that promotes financial integrity by articulating the operational and technical characteristics of payment stablecoins.

GBBC recommends anchoring customer identification program (CIP) obligations in the existence of a direct customer or account relationship with a PPSI. Ownership or use of a payment stablecoin in the secondary market, or interaction with a PPSI via a smart contract, should not alone constitute a customer relationship. Preserving this distinction helps prevent duplicative or impracticable identification requirements while ensuring the continued application of more extensive anti-money laundering/countering the financing of terrorism (AML/CFT) and sanctions obligations where appropriate.

GBBC further encourages FinCEN and the Agencies to preserve flexibility in how PPSIs fulfill identity-verification requirements. Digital identity solutions, verifiable credentials, and other innovative technologies should be permitted when they enable a PPSI to meet the relevant risk-based standard, without mandating a specific technology, provider, architecture, or verification method.

A technology-neutral, outcomes-based framework empowers PPSIs to adapt their compliance programs to their business models, technical architectures, customer relationships, and risk profiles, while assuring that PPSIs can reasonably identify and verify their customers.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

About GBBC:

GBBC is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

GBBC furthers adoption of digital technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chains, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), Capital Markets Risk Mitigation Framework (RMF), GBBC Digital Media, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).

Questions

1. Should any CIP requirement be extended to secondary market activity? If yes, in what circumstances? What would be the benefits and drawbacks of doing so?

GBBC does not recommend extending Customer Identification Program (CIP) requirements to secondary-market activity absent a direct account relationship between the person and the permitted payment stablecoin issuer (PPSI). A person's acquisition or use of payment stablecoins in the secondary market should not, in and of itself, trigger the PPSI's CIP. Where that person later establishes an account directly with the PPSI, CIP requirements would arise from that account relationship, regardless of how the payment stablecoins were originally acquired. The same is true of a person who approaches a PPSI to redeem a payment stablecoin. Redemption is a direct dealing between the holder and the issuer, and GBBC has previously recommended in its [response](#) to the FinCEN and OFAC joint proposed rule, *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements (Docket FINCEN-2026-0100)*, that attaching regulatory obligations to redemption as a risk-bearing activity. CIP would therefore apply to a redemption relationship, subject to procedures proportionate to the nature and duration of that relationship.

In an onchain secondary-market transaction, a PPSI may observe information such as wallet addresses, transaction hashes, asset amounts, timing, and transaction history without knowing the person or legal entity controlling the relevant address. Contract-layer controls likewise operate on identified addresses and cannot, by themselves, determine the identity of the person behind an unlisted wallet. Extending CIP on the basis of this technical interaction would require a PPSI to

identify persons with whom it has no direct relationship and for whom it may lack the information needed to verify identity. Consistent with its prior comments made in response to [Docket FINCEN-2026-0100](#), GBBC does not regard a payment stablecoin transfer as a transaction conducted or attempted by, at, or through a PPSI solely because the transfer interacts with the PPSI's smart contract.

Technical visibility and control should remain distinct from a customer relationship. A PPSI may possess the capability to monitor, block, freeze, or reject certain activity without maintaining an account for the person conducting that activity. The GENIUS Act imposes the obligation to maintain technical capabilities and the customer-facing Bank Secrecy Act obligations as separate duties, and the existence of the former does not itself establish the account relationship on which CIP depends. Treating these capabilities as sufficient to establish a customer relationship could turn the operation of a payment stablecoin into an open-ended obligation to identify downstream users.

This approach does not exempt secondary-market activity from the broader anti-money laundering and countering the financing of terrorism (AML/CFT) and sanctions frameworks. Sanctions compliance, suspicious activity reporting, transaction monitoring, block, freeze, and reject capabilities, and lawful-order compliance may still apply depending on the PPSI's legal obligations, available information, control mechanisms, and technical capabilities. GBBC, in its response to [Docket FINCEN-2026-0100](#), recommended extending block, freeze, reject, and lawful-order obligations to secondary-market activity where those obligations are tied to a PPSI's legal responsibility and technical capability. The distinction GBBC draws here is between obligations that operate on identified addresses and transactions, which a PPSI can discharge without knowing the person behind a wallet, and CIP, which depends on a relationship that allows the PPSI to collect and verify reliable customer information.

Broadly applying CIP requirements to secondary-market activity could result in duplicative identification efforts by regulated intermediaries that already maintain direct customer relationships. It may also compel PPSIs to seek information they are not equipped to obtain, or to rely on incomplete or inaccurate assumptions about wallet ownership. CIP is most effective when implemented through relationships that allow the PPSI to collect and verify reliable customer information, while other risk controls address issues arising at different stages of the payment stablecoin lifecycle.

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

The currently proposed definitions of “account,” “customer,” and “digital asset service provider” appropriately focus on the underlying relationship or financial activity, rather than treating interaction with blockchain infrastructure as independently determinative of regulatory status.

This approach is consistent with the [CFTC GMAC Digital Asset Markets Subcommittee's Digital Asset Classification and Taxonomy](#), which emphasizes classification based on objective characteristics and functions rather than the type of database, network, or technology supporting the asset. GBBC has similarly recommended definitions that attach regulatory obligations to relevant risk-bearing activities, including issuance, redemption, reserve management, custody, transferability, and control in its previous [response](#) (specifically to questions 5-7 of the request for comment section) to FinCEN and OFAC joint proposed rule, *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements* ([Docket FINCEN-2026-0100](#)).

THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

The proposed definitions of “account” and “customer” appropriately apply this functional distinction to CIP by linking the obligation to the relationship between the PPSI and the individual. Mere ownership or control of a payment stablecoin, participation in secondary-market activity, or interaction with a smart contract does not, by itself, establish such a relationship.

The definition of “digital asset service provider” also maintains substantive continuity with the [GENIUS Act](#). It distinguishes covered activities, such as exchange, transfer, custody, and financial services related to issuance, from expressly excluded infrastructure-layer activities, including protocol development, self-custodial software, transaction validation, distributed ledger operations, and certain peer-to-peer liquidity activities. This functional distinction should remain clear to ensure that technical participation in digital asset infrastructure is not classified as financial intermediation solely because it supports or interacts with payment stablecoin activity.

GBBC recommends the addition of new definitions or clarifications that would provide greater certainty as payment stablecoin business models and technologies evolve. Any new definitions should be consistent with the [GENIUS Act](#), technology-neutral, function-based, and distinguish financial intermediation from infrastructure-layer activity. They should also avoid assigning regulatory consequences solely based on the technology used and remain flexible enough to accommodate evolving market structures without merging distinct activities or relationships.

Where uncertainty relates to the application of an existing term rather than a genuinely distinct concept, non-exclusive examples or interpretive guidance may provide greater clarity while preserving flexibility.

5. Should the regulatory text explicitly discuss digital identity solutions or verifiable credentials? How could it best do so given the range of tools available on the market?

GBBC recommends technology-neutral recognition of digital identity solutions and verifiable credentials within the regulatory text. Such recognition would clarify that these tools may be used as documentary or non-documentary methods of identity verification when, as part of a PPSI's risk-based CIP, they enable the PPSI to form a reasonable belief that it knows the customer's true identity.

This approach would build on existing CIP treatment rather than establish a new verification standard. FinCEN and the Agencies have already recognized "electronic credentials" as a potential method of identity verification and acknowledge that newer digital identity tools vary significantly in design and trustworthiness, as discussed in the preamble accompanying proposed 31 CFR § 1033.220(a)(2)(ii). The final rule should therefore stress flexibility in determining which methods are appropriate for a particular PPSI and customer.

GBBC similarly recommended, in its June [response](#) to FinCEN's *Anti-Money Laundering and Countering the Financing of Terrorism Programs* proposed rule ([Docket FINCEN-2026-0034](#)), the express recognition of responsible innovative technologies, including digital identity and verifiable credential solutions, where they produce demonstrable AML/CFT outcomes such as improved customer due diligence and higher-quality information. GBBC has also supported technology-neutral frameworks that preserve flexibility and avoid treating any single technical method as the exclusive path to compliance.

Accordingly, any reference in the regulatory text should be permissive rather than prescriptive and should not specify a particular provider, credential type, architecture, or technical standard. More detailed considerations about reliability, governance, or specific implementations could be addressed in accompanying guidance, allowing expectations to progress alongside technical developments.

8. What, if anything, could be changed to make the proposed rule more conducive to industry innovation? Explain how any changes would positively or negatively impact PPSIs expected operations and illicit finance risk to the U.S. financial system.

GBBC recommends a customer identification framework that delivers clear compliance outcomes while allowing permitted payment stablecoin issuers (PPSIs) to determine how those outcomes are achieved. The final rule may clarify this principle by confirming that compliance does not depend on the use of any particular technology, vendor, architecture, credential, or verification method, provided the PPSI meets applicable CIP requirements and can reasonably believe it knows its customer's true identity.

This approach is consistent with the broader direction of U.S. AML/CFT policy. Section 6002(3) of the [Anti-Money Laundering Act of 2020](#) identifies a statutory purpose encouraging “technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism.” FinCEN’s April 2026 *Anti-Money Laundering and Countering the Financing of Terrorism Programs* ([Docket FINCEN-2026-0034](#)) proposal similarly urges financial institutions to evaluate technologies, including digital identity, blockchain monitoring and analytics, artificial intelligence, and application programming interfaces, while declining to require any particular technology because different tools may not be appropriate for every institution.

The final rule could therefore provide greater certainty that PPSIs may use new and evolving verification technologies (including digital identity and verifiable credentials, electronic credentials, automated verification tools, APIs, and combinations of documentary and non-documentary methods) where those tools satisfy the applicable risk-based verification standard. Treasury’s March 2026 Report to Congress on [Innovative Technologies to Counter Illicit Finance Involving](#)

[Digital Assets](#) examines digital identity, blockchain analytics, and other emerging compliance technologies, and encourages responsible adoption of tools that can improve the effectiveness of the AML/CFT framework. FinCEN expressly references that report in its April 2026 AML/CFT proposal, *Anti-Money Laundering and Countering the Financing of Terrorism Programs* proposed rule ([Docket FINCEN-2026-0034](#)), encouraging the responsible use of novel models, techniques, and strategies.

Consistent with GBBC's [prior comments](#) on AML/CFT modernization, innovative methods should be evaluated by their demonstrable compliance outcomes rather than their novelty or similarity to legacy processes. In its response, GBBC has identified relevant outcomes, including improved customer and counterparty due diligence, more effective identification of higher-risk activity, lowered false positives, improved SAR quality, and more useful information for law enforcement and national security agencies. This approach would also reduce the risk that institutions retain older processes primarily because supervisors are more familiar with them, rather than because they provide better compliance outcomes.

Operationally, this flexibility could enable PPSIs to integrate CIP into digital-native onboarding processes, adopt more efficient verification technologies, and update compliance infrastructure as technology evolves. It could also reduce unnecessary implementation costs and duplication, while allowing different PPSIs to select tools suited to their business models, technical architectures, customer relationships, and risk profiles. This approach aligns with GBBC's previous recommendation for risk-based, technology-neutral frameworks, which avoid designating any single technical method as the exclusive path to compliance.

Such flexibility should not reduce protection against illicit finance where the substantive CIP standard remains unchanged. PPSIs would remain responsible for collecting required identifying information, applying risk-based verification procedures, and forming a reasonable belief that they know their customers' true identities.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

A technology-neutral and outcomes-based framework would enable the CIP regime to evolve in parallel with payment stablecoin markets while maintaining its core financial integrity objective. This approach would also reflect the [Anti-Money Laundering Act of 2020](#)'s broader aim of encouraging technological innovation that improves the effectiveness of AML/CFT compliance.