BLOCKCHAIN ASSOCIATION, SUMMER MERSINGER

Proposal and Comment Information

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

Comment ID: FR-2026-0005-01-C15

Submitter Information

Organization Name: Blockchain Association

Organization Type: Organization

Name: Summer Mersinger

Submitted Date: 08/21/2026

Attached please find a comment from Blockchain Association on the Joint Proposed Rule Re Permitted Payment Stablecoin Issuer Customer Identification Program.

BLOCKCHAIN ASSOCIATION

August 21, 2026

Via electronic submission

The Honorable Jenna Casanova,
Acting Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
Post Office Box 39
Vienna, VA 22183

The Honorable Jonathan V. Gould
Comptroller of the Currency
Office of the Comptroller of the Currency
400 7th Street SW, Suite 1E-216
Washington, DC 20219

The Honorable Kevin Warsh, Chairman
Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

The Honorable Travis Hill, Chairman
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

The Honorable Kyle S. Hauptman, Chairman
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Re: Permitted Payment Stablecoin Issuer Customer Identification Program (FinCEN Docket FINCEN-2026-0101, RIN 1506-AB74; OCC Docket OCC-2026-0331, RIN 1557-AF53; Board Docket R-1885, RIN 7100-AH18; FDIC RIN 3064-AG28; NCUA Docket NCUA-2026-0793, RIN 3133-AG09)

Dear Director Casanova, Comptroller Gould, and Chairmen Warsh, Hill, and Hauptman:

The Blockchain Association ("BA") submits this letter in response to the request for comments by the U.S. Department of the Treasury's ("Treasury") Financial Crimes Enforcement Network ("FinCEN"), Treasury's Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the National Credit Union Administration ("NCUA") (collectively, "the Agencies") on their joint proposed rule implementing provisions of the Guiding and Establishing National Innovation for

U.S. Stablecoins Act ("GENIUS Act"). The relevant provisions of the GENIUS Act require that permitted payment stablecoin issuers ("PPSIs") maintain an effective customer identification program ("CIP"), 91 Fed. Reg. 37,234 (June 22, 2026).

BA is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for the digital asset economy.[1] BA endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can pave the way for a more secure, competitive, and consumer-friendly digital marketplace. BA represents member companies reflecting the wide range of the dynamic blockchain industry, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem. Many of those member companies are building, supporting, or deeply interested in stablecoin products in the United States.

Introduction and Executive Summary

BA shares FinCEN's and the federal government's interest in preventing the use of digital assets for illicit purposes. Many of BA's members are active and trusted partners of law enforcement and regulators across the globe, and they regularly take action to assist law enforcement in identifying and preventing money laundering and countering terrorism financing, even when doing so goes beyond their legal obligations.[2]

BA supports the proposed rule's core design choices. In particular, BA supports the Agencies' decision to apply a customer-identification framework to PPSIs that is generally comparable to the familiar frameworks applicable to other financial institutions that are subject to the Bank Secrecy Act ("BSA"). BA also strongly supports the proposal's decision to limit CIP obligations to primary-market relationships in which a PPSI interacts directly with a customer, rather than attempting to impose customer-identification obligations across downstream secondary-market activity. Consistent with that limitation, the proposal appropriately defines an "account" by reference to a "formal relationship" between a PPSI and a customer.

---

[1] *See* Blockchain Association, https://theblockchainassociation.org.

[2] *See* Letter from Blockchain Association to Director Julie Lascar, Department of the Treasury, re Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, 2 (Oct. 17, 2025) (describing, among other examples, Coinbase's law-enforcement training programs and partnership with the U.S. Marshals Service, member assistance to the U.S. Secret Service in seizing approximately $225 million in fraud proceeds, and Circle's board seat on the Illicit Virtual Asset Notification partnership).

The final rule nevertheless could be improved by more clearly defining the requirements of a PPSI-specific CIP, avoiding duplicative application of overlapping BSA requirements, and ensuring that PPSIs may use modern and interoperable methods to collect and verify customer information. Specifically:

- **Definition of "account":** The Agencies should clarify that the definition of "account" does not include: (1) situations where a PPSI satisfies a stablecoin holder's one-off redemption request; (2) data-processing or transmission activities, vendor and service-provider relationships, and other commercial partnerships or business arrangements; (3) non-stablecoin-related activities subject to other BSA requirements; or (4) redemptions processed through another regulated financial institution.

- **Definition of "digital asset service provider":** For entities that issue stablecoins and also act as digital-asset service providers, the Agencies should make clear that the CIP requirements imposed by the proposed rule do not extend to those entities' activities as digital-asset service providers.

- **Reliance and information collection:** BA supports allowing PPSIs to rely on customer identification performed by other federally regulated financial institutions that are subject to their own CIP requirements. But the final rule should provide that issuers are not responsible for the failures of other regulated financial institutions so long as the issuers' reliance on those institutions is reasonable (as other financial institutions subject to CIP requirements are allowed to do). The final rule should also clarify that issuers may receive and collect required customer-identification information electronically and indirectly, including, for example, by obtaining a customer's taxpayer-identification number from a third party. And the final rule should leave open the possibility of allowing PPSIs to rely on customer identification by state-regulated stablecoin issuers in the future to the extent those issuers are subject to similar CIP requirements.

- **Effective date:** The effective date should be coordinated with, and be the same as, the effective date of FinCEN's and the Office of Foreign Assets Control's ("OFAC") separate but closely related rulemaking implementing the GENIUS Act's directive to apply anti-money laundering, countering the financing of terrorism, and sanctions compliance obligations to PPSIs.

I. The Agencies should maintain the proposed rule's decision to extend CIP obligations to primary-market activity only, not secondary-market activity.

Proposed 31 C.F.R. § 1033.100 contains three defined terms—account, customer, and digital asset service provider—that the Agencies say are designed to clarify that an issuer's CIP obligations

extend to primary-market activity only, not secondary-market activity. 91 Fed. Reg. at 37,239-40. The preamble to the proposed rule explains that the Agencies consider primary-market activity to be a PPSI's direct interaction "with a user or holder of a payment stablecoin, such as when a PPSI engages in issuing, converting, redeeming, repurchasing, burning, and reissuing payment stablecoins, as well as providing associated services, such as providing custodial services." *Id.* at 37,238. The Agencies understand secondary-market activity to refer to "payment stablecoin activity that does not directly involve the PPSI as a party to the transaction other than via a smart contract." *Id.* The Agencies request input on whether CIP requirements should be extended to secondary-market activity. *Id.* at 37,244 (Question 1).

BA strongly supports the Agencies' decision to confine the proposed CIP requirements to primary-market customer relationships, where PPSIs maintain direct customer relationships and exercise meaningful operational control. That approach is also required by the GENIUS Act. The Act requires that PPSIs establish effective CIPs that verify the identities of *only* "account holders with the permitted payment stablecoin issuer." 12 U.S.C. § 5903(a)(5)(A)(v). The Act thus does not authorize the Agencies to impose CIP requirements on PPSIs for downstream secondary-market transfers involving stablecoins that have already been issued into circulation.

Nor would extending CIP obligations to secondary-market activity make sense from a policy standpoint. Compliance obligations are effective when they are applied at centralized points of control. With respect to stablecoin issuers, those centralized points of control are primary-market activities—such as issuance, redemption, reserve management, and fiat conversion—involving account holders with whom issuers have contractual relationships. In secondary-market transactions, by contrast, a PPSI often has no contractual relationship with the parties, no custody over the stablecoins, and no technical ability to identify the actors behind the transaction. PPSIs do not intermediate, facilitate, approve, or participate in secondary-market, peer-to-peer transfers between third-party wallets. In a typical transfer, the sender's wallet signs and broadcasts the transaction to the blockchain network; distributed validators then confirm and include the transaction in a block; and then the transaction settles without the PPSI's involvement, approval, or knowledge. The PPSI's smart contract executes pre-programmed, non-discretionary code that is triggered by the transacting third-party wallets. The smart contract does not identify the parties, conduct know-your-customer ("KYC") diligence, evaluate sanctions status in real time, or provide the issuer with a pre-settlement approval function.

Accordingly, the Agencies are correct in recognizing that "interaction with a smart contract does not currently result in a PPSI acquiring the kind of information needed to verify an identity," and in determining that imposing CIP requirements on PPSIs for all payment stablecoin transfers would result in "nearly impossible" and "global" regulatory obligations that could "cripple the

industry." 91 Fed. Reg. at 37,239. For those reasons, BA strongly supports the Agencies' decision to extend CIP obligations to primary-market activity only.

II. BA supports the Agencies' proposed definitions of "account," "customer," and "digital asset service provider," but the Agencies should clarify those definitions.

In proposed 31 C.F.R. § 1033.100(a)(1), the Agencies define an "account" as "a formal relationship" between a PPSI and a customer "established to provide or engage in services, dealings, or other financial transactions." 91 Fed. Reg. at 37,270; *id.* at 37,239. The Agencies propose defining a "digital asset service provider" as an entity that engages in the business of exchanging, transferring, or holding digital assets. 91 Fed. Reg. at 37,270; *id.* at 37,240. And the Agencies propose defining the term "customer," with certain exceptions, as a "person that opens a new account." 91 Fed. Reg. at 37,270; *id.* at 37,240.

BA generally supports the Agencies' proposed definitions of all three terms, and BA strongly supports the Agencies' decision to make the existence of a "formal relationship" between a PPSI and a customer the defining requirement for determining whether an "account" exists. The formal-relationship approach appropriately draws on established CIP rules for other federally regulated financial institutions such as banks, broker-dealers, and futures intermediaries; those rules similarly require the establishment of a formal relationship between a customer and the financial institution for the imposition of CIP obligations on the financial institution. *See* 31 C.F.R. §§ 1020.100(a)(1), 1023.100(a)(1), 1026.100(a)(1). As the Agencies recognize, carrying that established framework into the CIP rules for PPSIs promotes consistency and efficiency, as well as equal treatment of regulated financial institutions. 91 Fed. Reg. at 37,239. The Agencies should retain the formal-relationship requirement as the central criterion for determining when a customer creates an account with a PPSI.

Although BA supports the Agencies' proposed definitions of "account," "customer," and "digital asset service provider," the Agencies can clarify and improve those definitions in at least four ways. The Agencies should clarify in regulatory text or accompanying guidance that: (1) the definition of "account" does not include circumstances where a PPSI satisfies a one-off redemption request from a stablecoin holder; (2) a PPSI's data-processing and transmission activities, vendor and service-provider relationships, and other commercial partnerships or business arrangements do not give rise to a formal relationship that creates an "account"; (3) the definitions of "account" and "digital asset service provider" do not encompass non-stablecoin-related activities subject to other BSA requirements; and (4) redemptions by a party through another regulated financial institution do not make the party a "customer" or create an "account."

A. The Agencies should omit one-off redemptions from the definition of an "account."

The proposed rule provides an illustrative list of "services, dealings, or other financial transactions" that would establish the formal relationship between a PPSI and a customer needed to create an account. That illustrative list includes "[i]ssuing or redeeming a payment stablecoin" under proposed 31 C.F.R. § 1033.100(a)(1)(i). The Agencies should clarify that, although a PPSI has no obligation to satisfy one-off redemption requests by a non-account holder, if a PPSI chooses to do so, that transaction does not create an "account" within the meaning of the proposed CIP rules. *See* 91 Fed. Reg. at 37,244 (Question 4). This clarification would be consistent with how FinCEN has defined "accounts" for other relationships for purposes of CIP and customer due diligence regulations.

Clarifying that one-off redemptions from non-account holders do not establish a formal relationship between a customer and a PPSI would align the proposed rule with existing CIP regulations governing banks. In the banking context, the Agencies' rules provide that certain one-off transactions such as "check-cashing" or the "sale of a check or money order" do not establish a formal banking relationship. *See* 31 C.F.R. § 1020.100(a)(2)(i). In adopting those bank-specific regulations, the Agencies acknowledged that the rules applicable to formal accounts were not "intended to cover infrequent transactions such as the occasional purchase of a money order." Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090, 25,092-93 (May 9, 2003).

The Agencies should adopt the same approach here. PPSIs have no obligation to satisfy a one-off redemption request by a non-account holder, and in current practice, issuers generally satisfy redemption requests only from account holders. But if a PPSI chooses to allow a non-account holder who acquired stablecoins on the secondary market to make a one-off request that a PPSI redeem those stablecoins, that request would be similar to a purchase of a money order or cashing a check: In both situations, the counterparty is engaging in a discrete, one-off financial transaction rather than seeking to establish an ongoing formal relationship with a financial institution.

Importantly, even when satisfying a one-off redemption request, other KYC requirements would kick in. PPSIs would still be required to obtain basic identifying information about the party seeking redemption and to report suspicious and high-value transactions to comply with suspicious-activity monitoring and reporting requirements. And a PPSI would maintain its ability to decline to satisfy the one-off redemption request. In the limited and rare instances where a PPSI satisfies a one-off redemption request from a non-account holder, there is no need to apply the full CIP requirements to these sporadic requests. Doing so would be a paradigmatic example of an untailored burden that would contravene the GENIUS Act's directive that BSA obligations, including

those related to maintaining a CIP, be tailored to issuers' size and complexity. 12 U.S.C. § 5903(a)(5)(B); *see also* 91 Fed. Reg. at 37,238; *Michigan v. EPA*, 576 U.S. 743, 752-55 (2015) (federal agencies generally must consider costs of regulations).

B. The Agencies should clarify that data-processing and transmission activities, vendor and service-provider relationships, and other ordinary commercial partnerships or business arrangements do not create a formal relationship that creates an "account."

Among the illustrative list of "services, dealings, or other financial transactions" that would establish a formal relationship between a PPSI and a customer, the proposed rule includes "[o]ther activities that directly support" issuance or redemption, reserve management, or custody or safekeeping. 91 Fed. Reg. at 37,239 (discussing proposed 31 C.F.R. § 1033.100(a)(1)). The phrase "directly support" could be read (incorrectly) to encompass non-issuer activities by the PPSI, including, for example, providing technological services that facilitate stablecoin transactions or communicating transaction-related data concerning information such as wallet balances, transaction histories, or transaction status; engaging a vendor or service provider to provide market data, oracle services, blockchain infrastructure, analytics, or other technology services that support the PPSI's issuance, redemption, or reserve-management functions; or entering into other commercial partnerships or business arrangements that are not transactional or custodial.

One important example: A PPSI's engagement of a vendor or service provider—including a provider of market data, oracle services, blockchain infrastructure, analytics, or other technology services that support the PPSI's issuance, redemption, or reserve-management functions—is a commercial procurement relationship, not a relationship in which the PPSI "provide[s] or engage[s] in services, dealings, or other financial transactions" for the counterparty. The Agencies should confirm that vendor and service-provider relationships like these do not establish a "formal relationship" that creates an "account," and that the vendors are not "customers" of the PPSI, notwithstanding that the vendor's services may "directly support" activities enumerated in proposed 31 C.F.R. § 1033.100(a)(1).

To avoid any potential ambiguity, the Agencies should clarify that the definitions in the proposed rule do not include these kinds of activities, or other services that are not transactional or custodial. That clarification would accord with FinCEN's longstanding distinction between financial intermediation and providing technical infrastructure. FinCEN's money-transmitter regulations, for example, exclude entities that merely provide "delivery, communication, or network access services" to support money transmission. 31 C.F.R. § 1010.100(ff)(5)(ii)(A). FinCEN's 2019 virtual-currency guidance explains that suppliers of communications, hardware, or software tools are engaged in trade rather than money transmission if they do not accept and transmit value

themselves. *See* FinCEN, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 9, 20, 24 (May 9, 2019). Treating the use or provision of comparable technical infrastructure as the opening of a PPSI account would collapse the distinction between transmitting information and transmitting financial value.

C. The Agencies should clarify that the definitions of "account" and "digital asset service provider" do not encompass non-stablecoin-related activities subject to other BSA requirements.

Proposed 31 C.F.R. § 1033.100(a)(1)(v) identifies "[p]roviding services of a digital asset service provider" as an activity that creates a PPSI "account." 91 Fed. Reg. at 37,270. Proposed 31 C.F.R. § 1033.100(c), in turn, defines a "digital asset service provider" to encompass a broad range of activities that do not pertain to the issuance or redemption of a payment stablecoin, such as exchanging or transferring digital assets. *Id.* FinCEN should revise the definitions of "account" or "digital asset service provider" (or both) so that, in combination, they do not apply the proposed CIP rules to non-stablecoin-related activities that are subject to other BSA requirements.

A literal reading of the proposed definitions of "account" and "digital asset service provider" would seem to treat a customer of a digital-asset exchange, transfer, custody, or issuance business as an account holder subject to PPSI-specific CIP requirements if the same legal entity is also a PPSI. That result would extend beyond the GENIUS Act's targeted directive that a PPSI maintain a CIP identifying and verifying only "account holders with the permitted payment stablecoin issuer." 12 U.S.C. § 5903(a)(5)(A)(v).

In the GENIUS Act, Congress also preserved a PPSI's ability to conduct authorized digital-asset-service-provider activities and made those activities subject to "all other Federal and State laws." 12 U.S.C. § 5903(a)(7)(B). Congress therefore recognized that a PPSI might also be a digital-asset service provider, but Congress did *not* provide that every customer using those different kinds of services would become an account holder under the rules governing the PPSI's CIP. The Agencies should therefore recognize that a PPSI's authorization to act as a digital-asset service provider does not, without more, convert every customer of that business line into an "account" holder with the issuer in its PPSI capacity.

Relatedly, the Agencies should further clarify that a PPSI's CIP obligations do not extend to any other lines of business the entity might have that are subject to different BSA obligations. Chapter X assigns different BSA obligations to different categories of financial institutions and activities. The Agencies recognize that banks, broker-dealers, mutual funds, futures commission merchants, and introducing brokers are subject to institution-specific CIP rules, and that although money transmitters are not subject to a general CIP requirement, they remain subject to AML-

program, transaction-specific identification, registration, reporting, and recordkeeping requirements. 91 Fed. Reg. at 37,236. Applying CIP requirements to a PPSI's non-payment-stablecoin business lines would either duplicate an existing CIP requirement or undermine FinCEN's decision to regulate that activity through a different combination of AML/CFT controls.

Without these clarifications, PPSIs that offer other BSA-regulated services would face overlapping registration, reporting, and supervisory requirements that are inconsistent with the GENIUS Act's objective of establishing a coherent, tailored framework for PPSIs. *See* Blockchain Association, Comment on FinCEN and OFAC Joint Notice of Proposed Rulemaking Regarding PPSI AML/CFT and Sanctions Compliance Program Requirements 12 (June 9, 2026). And the proposed rule's approach would treat otherwise similar digital-asset (or other) service providers differently. A customer engaged in digital-asset trading, for example, could become subject to the full CIP requirements for PPSIs merely because the service provider also happens to issue a payment stablecoin, even though the same service offered by a non-PPSI money transmitter would not carry a general CIP obligation. For these reasons, the Agencies should ensure that the final rule does not impose PPSI-specific CIP requirements on the accounts of non-stablecoin-related businesses.

D. The Agencies should clarify that redemptions by a party through another regulated financial institution do not make the party a "customer" or create an "account."

As discussed, under proposed 31 C.F.R. § 1033.100(a)(1)(i), "[i]ssuing or redeeming a payment stablecoin" is listed among the "services, dealings, or other financial transactions" that the proposed rule states would create an "account" between a PPSI and a customer. 91 Fed. Reg. at 37,270. The proposed rule acknowledges that parties may redeem payment stablecoins through another regulated financial institution. *Id.* To guard against the creation of customer relationships through indirect redemptions, the Agencies have proposed excluding from the definition of "customer," as relevant here, a "person acquiring or redeeming a payment stablecoin from a means other than directly from or directly to the permitted payment stablecoin issuer." *Id.* The definition of "account" likewise excludes "payment stablecoin activity that does not directly involve the permitted payment stablecoin issuer as a party to the transaction other than via smart contract." *Id.*

BA supports the Agencies' proposal to exclude a party's indirect redemption through another regulated financial institution from the definitions of "account" and "customer." But the Agencies' final rule should make explicit that a redemption request is not "directly to" a PPSI and does not "directly involve" a PPSI "as a party" when a cryptocurrency exchange or other digital-asset service provider submits, on behalf of a customer, a redemption request to the PPSI either: (1) through off- and on-ramps to the PPSI's platform; or (2) through the exchange's or service

provider's own account(s) with the PPSI. In those circumstances, the PPSI's redemption should be deemed to "directly involv[e]" the cryptocurrency exchange or digital-asset service provider, not the exchange's or provider's customer. Even if the PPSI receives information about the downstream customer, that customer should not be deemed to be the PPSI's "customer" or treated as having an "account" with the PPSI for purposes of triggering the PPSI's CIP requirements. That approach would be consistent with FinCEN's proposal to limit "customer" relationships to direct, formal relationships between a customer and the PPSI, and it would also support FinCEN's objective of making the BSA more efficient and effective by reducing unnecessary redundancies across multiple BSA-regulated institutions involved in a redemption or other transaction.

III. BA supports the Agencies' proposal to impose generally the same customer-identification requirements for PPSIs as FinCEN imposes on other financial institutions.

The Agencies propose imposing CIP obligations on PPSIs that are "comparable to existing CIP requirements for other financial institutions," including requirements that PPSIs maintain a written CIP, implement risk-based customer-identity-verification procedures, and maintain customer-identifying records. 91 Fed. Reg. at 37,238, 37,241-43. BA supports the Agencies' proposal to impose customer-identification requirements on PPSIs that are similar to the requirements imposed on other federally regulated financial institutions. BA agrees that imposing equivalent requirements on both sets of institutions would "increase the effectiveness and efficiency of CIP programs" and facilitate PPSIs' reliance on other institutions' CIPs. *Id.* at 37,238. In the final rule, however, the Agencies should clarify that: (1) issuers are not responsible for the failures of other regulated financial institutions; and (2) issuers can receive the required customer-identification information electronically and indirectly. This would be consistent with how reliance regulations apply to other financial institutions subject to CIP requirements. In the future, the Agencies should consider a mechanism for allowing reliance by PPSIs on state issuers that are subject to CIP requirements that are substantially similar to the requirements applicable to federally regulated institutions.

A. The Agencies should clarify that PPSIs are not responsible for failures of other regulated financial institutions.

To facilitate coordination and eliminate duplicative efforts between PPSIs and other regulated financial institutions, the Agencies should revise the proposed rule's provisions concerning reliance on other financial institutions. The Agencies should ensure that, when a PPSI reasonably relies on another regulated financial institution's CIP procedures and otherwise complies with the proposed rule's reliance provisions, the PPSI will not be held responsible for the relied-upon institution's failure to adequately fulfill its own CIP responsibilities.

The proposed rule allows a PPSI to rely on another federally regulated financial institution's performance of a customer-identification procedure if the relied-upon institution is subject to an AML/CFT program with CIP requirements, the relied-upon institution certifies annually that it has implemented an AML/CFT program and will perform the specified requirements, and reliance by the PPSI is otherwise reasonable under the circumstances. 91 Fed. Reg. 37,243 (discussing proposed 31 C.F.R. § 1033.220(a)(6)). Under the proposal, a PPSI would still maintain the ultimate responsibility for its CIP compliance. *Id.* The final rule should clarify that if an issuer complies with the three reliance requirements above, including that the issuer's reliance is reasonable under the circumstances, then the issuer will not be responsible for the failure of another institution to adequately fulfill its CIP responsibilities.

That approach would align the final rule with the rules governing CIPs for banks. *See* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090, 25,104 (May 9, 2003) (a "bank will not be held responsible for the failure of the other financial institution to adequately fulfill the bank's CIP responsibilities, provided the bank can establish that its reliance was reasonable and that it has obtained the requisite contracts and certifications"). Here, by contrast, the preamble to the Agencies' proposed rule states that reliance on another federally regulated institution "would not change a PPSI's CIP obligation" and that "the PPSI would remain responsible for its compliance." 91 Fed. Reg. at 37,243. That could be read to leave open the possibility that PPSIs, unlike banks, could be held liable when another institution fails to adequately fulfill its CIP responsibilities, even when the PPSI reasonably relied on that institution and complied with the PPSI's own obligations and the provisions of the proposed rule allowing PPSIs to rely on other federally regulated institutions as part of the PPSI's CIP. *Id.* at 37,242-43. There would be no rational justification for that disparate treatment of banks and PPSIs.

B. The Agencies should clarify that issuers can receive the required customer-identification information electronically and indirectly.

Proposed 31 C.F.R. § 1033.220(a)(2)(i) requires that a PPSI obtain identifying information "from the customer." 91 Fed. Reg. at 37,271. The Agencies should confirm in the final rule that a customer need not enter, upload, or transmit identifying information and supporting materials directly to the PPSI. Rather, the Agencies should clarify that a PPSI may receive the required information and supporting materials electronically and indirectly through, for example, a customer-controlled digital wallet, a secure application-programming interface, a verifiable credential, or another reliable electronic solution, provided that the information is transmitted with the customer's authorization or otherwise lawfully obtained.

That would be consistent with longstanding CIP guidance permitting electronic credentials, which allows information regarding one joint account holder to be furnished by another account holder acting on that person's behalf, and permits agents and other financial institutions to collect required customer information and perform CIP functions. *See* FinCEN, *FAQs: Final CIP Rule 10* (Jan. 2004); FinCEN, *Interagency Interpretive Guidance on Customer Identification Program Requirements, Customer Notice FAQs 1-2 & Reliance FAQ 1* (Apr. 28, 2005). It would also accord with the proposal's risk-based and technology-neutral structure, which recognizes the rise and prevalence of digital-identity tools and electronic credentials. 91 Fed. Reg. at 37,234, 37,242.

Relatedly, the Agencies should confirm that PPSIs may obtain a customer's taxpayer-identification number from a third-party source and verify it with the customer, rather than collecting the number directly from the customer at account opening. That would be consistent with the Board and FinCEN's CIP Exemption Order for Banks issued in July 2025. *See* FinCEN Order (July 31, 2025), https://www.fincen.gov/system/files/2025-08/CIP-TIN-Exemption-Order-Board-only-508.pdf. There, the Board and FinCEN observed a "significant expansion in ways that consumers access financial services" coupled with a rise in customer reluctance to provide taxpayer-identification numbers, especially in non-face-to-face transactions, due to concerns about data breaches, privacy, and identity theft. *Id.* at 4. The Board and FinCEN further acknowledged that "[r]eliable alternative processes for verification—which allow the bank to form a reasonable belief that it knows the true identity of each customer—are more prevalent today . . . meaning there could be circumstances in which such processes produce an equivalent or more reliable outcome when banks are permitted the flexibility to change their method of [taxpayer-identification number] collection based on the bank's assessment of the relevant risks." *Id.* at 7. Allowing PPSIs to obtain taxpayer-identification numbers from third-party sources would likewise provide "an efficient and effective means" of identity verification with "little risk" that the PPSI does not know the customer's identity. *Id.* at 6.

C. The Agencies should leave open the possibility of enabling reliance on state-regulated financial institutions' customer-identification programs in the future.

To further facilitate coordination and eliminate duplicative efforts between PPSIs and other regulated financial institutions, the Agencies should leave open the possibility of allowing PPSIs to rely on state-regulated financial institutions' CIP procedures just as the proposed rule already contemplates for federally regulated financial institutions.

The proposed rule would not allow PPSIs to rely on customer-identification procedures of a State-qualified payment stablecoin issuer ("State Issuer"). 91 Fed. Reg. 37,243. But as FinCEN acknowledges, that distinction "create[s] a disparity" between state and federally regulated issuers. *Id.* PPSIs "would not be able to rely on a procedure performed" by a State Issuer because "such

issuers are not overseen by a Federal functional regulator," whereas a State Issuer could rely on a procedure performed by a federally regulated PPSI. *Id.*

In enacting the GENIUS Act, Congress deliberately preserved a role for State supervision alongside the federal framework, reflecting the longstanding tradition of a dual banking system overseen by State and federal regulators. Section 4(c) of the GENIUS Act allows an issuer with a consolidated outstanding issuance of no more than $10 billion to opt into regulation under a state's regulatory regime, provided that the regime is "substantially similar" to the federal regulatory framework. *See* 12 U.S.C. § 5903(c). To implement that provision, Treasury has issued a proposed rule that would establish broad-based principles for determining when a state-level regulatory regime is substantially similar to the federal regulatory framework. *See* GENIUS Act Broad-Based Principles for Determining Whether a State-Level Regulatory Regime Is Substantially Similar to the Federal Regulatory Framework, 91 Fed. Reg. 16,844 (Apr. 3, 2026).

Treasury expects that all "BSA and sanctions compliance provisions" outlined in Section 4(a)(5) of the GENIUS Act "will necessarily apply to [State Issuers]" either through "uniform" state requirements or state laws that incorporate by reference federal BSA requirements, although Treasury expects to address such requirements "in a forthcoming rulemaking." 91 Fed. Reg. at 16,851-52. Once Treasury finalizes its proposed rule(s) implementing GENIUS Act Section 4(c), the Agencies should consider allowing PPSIs to rely on customer-identification procedures conducted by State Issuers if State Issuers will be subject to CIP or CIP-like requirements that are substantially similar to the applicable requirements for federally regulated institutions. That would further reduce duplicative CIP responsibilities, avoid fragmentation from State regulatory oversight that could undermine the development and usage of payment stablecoins, and help ensure that the Agencies' rules are consistent with the role that the GENIUS Act preserves for State supervision.

IV. The Agencies should maintain flexibility in how a PPSI verifies a customer's identity.

Proposed 31 C.F.R. § 1033.220(a)(2)(ii) requires PPSIs to adopt procedures for verifying a customer's identity using information the PPSI has collected about the customer. 91 Fed. Reg. at 37,242. The proposal recognizes the interest in "leveraging verifiable credentials and digital identity as part of account opening procedures," and proposes "maintaining the flexibility . . . relating to how a PPSI verifies a customer's identity" so that a PPSI can "assess its comfort level with the trustworthiness of various tools and take into consideration variation in tools and differences in risk." *Id.* The Agencies thus did not propose "regulatory text related to verifiable credentials and digital identities," but the Agencies requested comment on this approach. *Id.*; *see also* 91 Fed. Reg. 37,244 (Question 6) (asking about the "benefits and risks of using digital identity solutions or verifiable credentials as part of verifying customers' identities").

BA supports allowing issuers the flexibility to identify the best tools for ascertaining a customer's identity. That approach would allow, for example, the use of zero-knowledge proof ("ZKP") technologies through which customers provide cryptographic proof that they satisfy customer-identification predicates without transmitting the underlying personal data to the PPSI. Upon transmission, the PPSI does not receive the customer's raw identifying information but rather a verifiable proof that is mathematically sound and auditable. Such ZKP technology can still enable PPSIs to form a reasonable belief that they know the true identity of their customer in even more reliable ways than certain traditional methods, like comparisons against a public database.

V. The Agencies should coordinate the effective date with the closely related PPSI AML/CFT NPRM.

The Agencies propose that CIP requirements would become effective 12 months after the issuance of the final rule. 91 Fed. Reg. at 37,244. The compliance date for this rule, which "represents one piece of a comprehensive regulatory framework for PPSIs set out in the GENIUS Act," 91 Fed. Reg. at 37,237, should account for the effective date of FinCEN's and OFAC's separate but closely related rulemaking implementing the GENIUS Act's directive to apply anti-money laundering, countering the financing of terrorism, and sanctions compliance obligations to PPSIs, *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"). As the Agencies recognize, the proposed requirements in this rulemaking will be codified in a new part 1033 of Chapter X, which itself will not be finalized until FinCEN and OFAC finalize the PPSI AML/CFT NPRM. 91 Fed. Reg. at 37,237. Moreover, the proposed CIP requirements rely on and incorporate several definitions—including, for example, the definition of a "permitted payment stablecoin issuer"—that were proposed in the PPSI AML/CFT NPRM. *Id.*

Given this proposed rule's dependence on the PPSI AML/CFT NPRM, the compliance date for any final rule in this rulemaking should be coordinated with and have the same effective date as the PPSI AML/CFT NPRM. A staggered or uncoordinated set of effective dates would force issuers to build compliance programs in a shifting and inconsistent environment, incurring duplicative costs with no corresponding benefit to AML/CFT objectives.

Conclusion

We appreciate the opportunity to comment on the Agencies' proposal. BA supports the Agencies' decision to apply the existing CIP frameworks applicable to other BSA-regulated institutions to PPSIs, and BA urges the Agencies to adopt the proposed rule with the clarifications and revisions described above. BA welcomes the opportunity to meet with the Agencies and their staff

to address any questions regarding this comment letter. Please direct any questions to Ashok Pinto, Vice President, Legal & Government Relations, at ashok@theblockchainassociation.org.

Respectfully submitted,

/s/ Summer K. Mersinger
Summer K. Mersinger
Chief Executive Officer