August 21, 2026

Via *regulations.gov*

Regulatory and Strategic Affairs Division
Financial Crimes Enforcement Network
P.O. Box 39 Vienna, VA 22183

Re: Customer Identification Program Requirements for Permitted Payment Stablecoin Issuers; Docket No. FINCEN-2026-0101

DeFi Education Fund ("DEF") and Solana Policy Institute ("SPI") respectfully submit the following comments in response to the joint Notice of Proposed Rulemaking ("NPRM") issued by the Financial Crimes Enforcement Network ("FinCEN") and 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 (collectively, "the Agencies") concerning customer identification program ("CIP") obligations applicable to permitted payment stablecoin issuers ("PPSIs") under the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("GENIUS Act").[1]

DEF is a U.S.-based nonpartisan research and advocacy nonprofit that advocates for sound policy for decentralized finance ("DeFi"), educates lawmakers about the technical workings and benefits of DeFi, and protects the rights of DeFi developers and users.

SPI is a U.S.-based nonpartisan nonprofit focused on educating policymakers on how decentralized networks like Solana are the future of the digital economy and why those building on and using them need legal certainty to flourish.

DEF and SPI appreciate FinCEN and the Agencies' efforts to implement the GENIUS Act in a manner consistent with both national security objectives and the realities of decentralized technology. We support robust, effective anti-money laundering/countering the financing of terrorism ("AML/CFT") enforcement directed toward appropriate actors. Congress adopted a carefully targeted statutory framework in the GENIUS Act that properly imposes AML, Bank Secrecy Act ("BSA"), and CIP obligations on PPSIs — the intermediaries that control stablecoin issuance and intermediate customer transactions. Separately, Congress defined "digital asset service provider" ("DASP") and expressly excluded distributed ledger protocols, immutable and self-custodial software interfaces, validators, and liquidity pool participants.[2] Those provisions support a final rule that focuses obligations on the PPSI and does not use the account definition to erase Congress's DASP exclusions.

---

[1] Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37,234 (Jun. 22, 2026).
[2] 12 U.S.C. § 5901(7)(B).

In many respects, the NPRM reflects that statutory structure. In particular, the distinction between "primary market" and "secondary market" activity appropriately aligns CIP obligations with the actors best positioned to implement them, PPSIs. Other aspects, however, would benefit from additional clarification to ensure appropriate treatment for secondary market activities, decentralized networks, DeFi protocols, and non-custodial infrastructure providers.

Consistent with our prior comment letters regarding implementation of the GENIUS Act,[3] the proposed rulemaking should be guided by three overarching principles: (1) obligations should attach to entities with custody of customer funds or technical control over funds, (2) requirements should be function-based and technology-neutral rather than tied to a particular architecture, and (3) the final rule should remain anchored in the statutory text of the GENIUS Act and existing FinCEN guidance.

Those principles support robust PPSI-level compliance without converting CIP obligations into an indirect mechanism to regulate infrastructure, DeFi protocols, self-custody tools, validators, front-end interfaces, or liquidity providers that lack customer relationships or control over user assets. DEF and SPI urge FinCEN and the Agencies to avoid creating a standard that treats mere connection to network activity or technical communication of transactions as sufficient to trigger CIP obligations, and instead maintain a framework grounded in custody and control over customer assets. Upholding those principles in the final rule will promote legal certainty, preserve the statute's carefully calibrated balance, and reduce the risk of unintended consequences for open blockchain infrastructure and peer-to-peer activity.

I. Executive Summary

- **The Final Rule Should Ensure CIP Obligations Remain Tied to PPSI Accounts and Direct Relationships:** The GENIUS Act places CIP obligations only on PPSIs, a narrow, regulator-approved category of stablecoin issuers that FinCEN and the Agencies expect to number just 50 nationwide.[4] The NPRM appropriately defines "customer" by reference to a direct relationship with a PPSI, excluding secondary-market activity that does not directly involve the PPSI. Non-custodial software developers, front-end operators,

[3] DEF and SPI incorporate by reference the November 4, 2025 Response to the Department of Treasury's Advance Notice of Proposed Rulemaking on the Implementation of the GENIUS Act ("Nov. 2025 Comment Letter") https://www.defieducationfund.org/wp-content/uploads/2025/11/GENIUS-Act-Implementation-Comments-11-04-25.pdf and the June 9, 2026 comment letter on the Notice of Proposed Rulemaking regarding Permitted Payment Stablecoin Issuer AML/CFT and Sanctions Compliance Program Requirements, Docket No. FinCEN 2026-0100, https://www.defieducationfund.org/wp-content/uploads/2026/06/DeFi-Education-Fund-and-Solana-Policy-Institute.pdf. DEF further incorporates its October 17, 2025 Response to the Department of Treasury's Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, Docket No. TREAS-DO-2025-0070 ("Oct. 2025 RFI Response"), https://www.defieducationfund.org/wp-content/uploads/2025/10/2025-10-16-DEF-Treasury-RFI-Response.pdf.

[4] NPRM at 37,246.

blockchain validators, self-custody wallet providers, and other infrastructure providers should not be treated like intermediaries merely because non-custodial software or technology is used in connection with a PPSI-regulated stablecoin. The final rule should preserve this statutory perimeter as proposed in the NPRM.

- **The DASP Definition Should Not Be Expanded to Reach Statutorily-Excluded Non-Custodial Infrastructure Activities**: The GENIUS Act excludes distributed ledger protocols, self-custodial software interfaces, transaction validators, and liquidity pool participants from the DASP definition.[5] The NPRM's proposed DASP definition rightly preserves these exclusions[6] and remains consistent with FinCEN's 2019 CVC Guidance, which similarly declined to treat unhosted wallets and decentralized exchanges as money transmitters absent "total independent control" over user assets.[7] The final rule should consistently incorporate these statutory exclusions and should avoid any interpretation of intermediary status that would directly impose CIP obligations on actors who lack the technical capability to exercise custody or control.

- **CIP Obligations Should Not Transform Self-Custody Wallets or Secondary Market Interactions Into PPSI Accounts**: FinCEN and the Agencies should clarify that a self-custody wallet address, smart contract address, or interaction with a PPSI-issued stablecoin does not by itself create an "account" relationship between the wallet holder and the PPSI. Such a clarification is consistent with the NPRM's inclusion of the "formal relationship" threshold in its definition of an account.[8] Treating every address that holds or transfers a payment stablecoin as a PPSI "account" would collapse the statutory distinction between primary market customer relationships and secondary market activity, and would conflict with the GENIUS Act's protections for self-custody and direct peer-to-peer transfers.

II. CIP Obligations Should Remain on PPSIs and Primary Market Activity, Not on Secondary Markets or DeFi

CIP requirements should remain on primary market activity and not be extended to secondary-market activity merely because a PPSI-issued stablecoin is held or transferred, as the drawbacks of doing so are severe and no offsetting benefit exists (Question 1). One of the most constructive aspects of the NPRM is its recognition of the distinction between "primary market" and "secondary market" activity.[9] The proposal appropriately cabins compliance obligations to the primary market context, where PPSIs maintain direct relationships with users and control

[5] 12 U.S.C. § 5901(7)(B).
[6] NPRM at 37,240.
[7] FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 29, 2019) at 16, 23-24 (exempting unhosted wallets and decentralized exchanges from money transmitter status).
[8] NPRM at 37,239.
[9] NPRM at 37,238.

customer assets, and correctly focuses customer identification obligations on those intermediary relationships. This approach is well-grounded in the statutory text: as stated in the NPRM, "purely secondary market payment stablecoin activity does not form a formal relationship between a PPSI and a payment stablecoin user or holder."[10] Unlike traditional financial institutions, PPSIs generally lack direct customer, custodial, or account-based relationships with secondary market users, and are not able to collect customer or transactional information as conventional BSA-regulated intermediaries do.

FinCEN's decision not to impose generalized CIP obligations on non-customer secondary market activity is well calibrated to both the statutory framework and the operational realities of decentralized systems. That approach is also prudent given longstanding concerns that overly expansive reporting obligations can generate substantial volumes of low-value reporting while imposing significant compliance burdens with no corresponding law enforcement benefit.[11] This assessment should be preserved without qualification in the final rule.

Extending CIP obligations to secondary markets would carry the following drawbacks:

- **Operationally Infeasible:** As stated in the NPRM, "interaction with a smart contract does not currently result in a PPSI acquiring the kind of information needed to verify an identity," and issuers have only a limited ability to collect customer information on the secondary market.[12] Imposing CIP obligations on the secondary market would be "nearly impossible for PPSIs to implement and could potentially cripple the industry."[13] A workable CIP framework must track a direct PPSI relationship and the practical ability to obtain and verify required information.

- **Compliance Burdens and Privacy Risks:** Extending CIP obligations to secondary markets would significantly increase compliance burdens and risks related to privacy and data security, including unnecessary honeypots of sensitive personal information. Blockchain analytics and risk-based review of reasonably available information are more tailored tools than blanket user identification.

- **Statutory Overreach:** The GENIUS Act's CIP mandate is expressly tied to "account holders with the permitted payment stablecoin issuer."[14] Secondary market participants, including liquidity pool participants, decentralized exchange users, and peer-to-peer transferors, are not account holders. Extending CIP to them, whether directly or through the back door of PPSI compliance programs, would exceed GENIUS's statutory mandate and nullify those exclusions. Consistent with *Loper Bright Enterprises v. Raimondo*,

[10] NPRM at 37,240.
[11] *See* Modernizing the BSA for Financial Crime in the 21st Century, Hearing Before Subcommittee on Nat'l Sec., Illicit Fin., and Int'l Fin. Insts., 119 Cong. 2 (2026) (Statement of Nicholas Anthony).
[12] NPRM at 37,239.
[13] *Id*.
[14] 12 U.S.C. § 5903(a)(5)(A)(v).

courts reviewing agency action will independently assess whether regulations are consistent with the governing statute.[15] The final rule should therefore preserve the NPRM's proposed DASP definition exclusions rather than adopt interpretations that could narrow the framework Congress established.

- **Contrary to FinCEN Guidance and Congressional Intent:** Extending CIP obligations to the secondary market would be inconsistent with FinCEN's 2013 and 2019 Guidance on CVCs,[16] which explains that BSA obligations attach to those who accept or transmit funds on behalf of others, an activity that most secondary market participants do not engage in. It would also cut against congressional intent. During consideration of the GENIUS Act, the Senate Banking Committee observed that broader AML obligations applicable to DASPs and secondary market activity would be more appropriately addressed through future market structure legislation,[17] suggesting that Congress intentionally declined to impose comprehensive CIP obligations on secondary market participants through the GENIUS Act itself.

The final rule should affirmatively state that secondary-market activity does not create an account or customer relationship with a PPSI or trigger CIP obligations.

III. The Definitions of Account, Customer, and DASP Should Preserve the GENIUS Act's Non-Custodial Infrastructure Exclusions

The "account" and "customer" definitions should be refined to confirm they reach only primary market, intermediated activity, and the rulemaking should remain consistent with the "DASP" definition exclusions Congress already enacted (Question 2).

The proposed definition of "account" as a "formal relationship between a PPSI and a customer, established to provide or engage in services, dealings, or other financial transactions" appropriately limits the account definition to intermediated customer relationships.[18] The proposed exclusions, clarifying that purely secondary market payment stablecoin activity does not form a formal relationship, and that ownership or control of a PPSI's payment stablecoins alone does not constitute an account, are essential and should be retained and strengthened.[19]

---

[15] *Loper Bright Enterprises v. Raimondo*, 603 U.S. 369 (2024).
[16] *See* FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,* FIN-2013-G001 (Mar. 18, 2013) ("The term 'money transmission services' means 'the acceptance of currency, funds, or other value … and the transmission of currency, funds, or other value…." (emphasis added)); *see also* FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001* (May 9, 2019).
[17] *See* Senate Comm. on Banking, Hous., and Urb. Affairs, *Myth vs. Fact: The GENIUS Act*, Senate Comm. on Banking, Hous., and Urb. Affairs (May 8, 2025), https://www.banking.senate.gov/newsroom/majority/myth-vs-fact-the-genius-act (stating that "other comprehensive AML provisions for digital assets, digital asset service providers, and secondary markets, would be more appropriate for a broader discussion, and potentially enacted as a part of a crypto market structure bill").
[18] NPRM at 37,239.
[19] NPRM at 37,240.

FinCEN and the Agencies also propose providing an "illustrative list of activities" that fall within the proposed account definition.[20] Those examples include activities such as issuing and redeeming a payment stablecoin and managing, holding, or custodying reserve assets for a payment stablecoin, among other activities.[21] Each of these enumerated activities requires control of customer funds or execution of transactions on behalf of customers to reach the threshold of an account. Should FinCEN and the Agencies include an illustrative list of activities in the final rulemaking, it should include an explicit acknowledgement that non-controlling, non-custodial developers or participants are not included.

Similarly, the final definition of a "customer" should retain the NPRM's proposed exclusion for "a person acquiring or redeeming a payment stablecoin from a means other than directly from or directly to the PPSI."[22] The final rule should make explicit that secondary market purchasers, holders, and transferors of payment stablecoins are not "customers" of the PPSI for CIP purposes, regardless of whether the stablecoin was originally issued by that PPSI.

With respect to "digital asset service provider," the proposed definition is largely consistent with the GENIUS Act's statutory definition and, importantly, its exclusions. To confirm that consistency, the final rule should clarify that the DASP definition's three proposed modifications — substituting the GENIUS Act's own definition of "person," and incorporating its definitions of "monetary value" and "distributed ledger protocol" — are not intended to modify the statutory exclusions in any way.[23]

IV. "Formal Relationship" Should Remain Part of the "Account" Definition, With Guidance Confirming Secondary Market Activity Falls Outside It

The final rule should also retain the requirement that there be a "formal relationship" as part of the definition of an "account." However, FinCEN and the Agencies should clarify the hallmarks of a "formal relationship" through guidance and confirm that secondary market interactions do not meet that standard (Question 3).

The "formal relationship" language is the same formulation used in CIP rules already applicable to banks, broker-dealers, mutual funds, and futures commission merchants,[24] and retaining it allows PPSIs to rely on the existing regulatory frameworks and interagency guidance interpreting that standard.

Hallmarks of a "formal relationship" between a PPSI and a user could include: a direct, affirmative act by the user to open an account or engage in a primary market transaction with the PPSI (such as issuance or redemption of a payment stablecoin directly with the PPSI); a

[20] NPRM at 37,239.
[21] NPRM at 37,239.
[22] NPRM at 37,240.
[23] NPRM at 37,240.
[24] *See* NPRM at 37,239 n.58.

contractual or terms-of-service relationship between the PPSI and the user; the PPSI's collection of identifying information from the user in connection with the account opening or primary market transaction; and the PPSI's exercise of custody, control, or operational authority over the user's assets or transactions. Critically, a "formal relationship" insinuates that a PPSI serves as an intermediary.[25]

Conversely, the final rule should reflect that where no direct PPSI-customer relationship exists, there is no "formal relationship." This distinction is critical in decentralized systems, where there are no custodial, customer, or account-based relationships between developers and end users. For example, the following actions would not constitute a "formal relationship": acquiring a payment stablecoin on a secondary market exchange or through a peer-to-peer transfer; holding or transferring a payment stablecoin without any direct interaction with the PPSI; interacting with a PPSI-issued stablecoin solely through a smart contract, without any direct relationship with the PPSI; and using a self-custody wallet to hold or transfer a payment stablecoin.[26]

FinCEN and the Agencies should provide examples or attributes of a formal relationship in guidance. Guidance would reduce compliance uncertainty for PPSIs and help ensure that the "formal relationship" standard is not interpreted expansively to sweep in secondary market users, self-custody wallet holders, or DeFi protocol participants. Should FinCEN and the Agencies adopt an alternative concept for the "account" definition, it should be defined to affirmatively exclude secondary market activity and peer-to-peer transactions, consistent with the GENIUS Act's statutory framework.

V. FinCEN and the Agencies Should Address Digital Identity Solutions and Verifiable Credentials in the Final Rule

While digital identity solutions can offer meaningful benefits relative to traditional KYC, they also raise certain risks. Digital identity solutions offer efficiency and speed gains over traditional CIP methods; create more accessible identity verification systems for individuals without traditional identity documents; and potentially enhance fraud protection through the incorporation of biometric verification, liveness detection, and other anti-fraud features. With further innovation, the adoption of privacy-preserving verifiable credentials and zero knowledge proofs could enable identity verification without requiring the disclosure of unnecessary personal information to the verifying institution. These benefits, however, do not overcome the

[25] *See* NPRM at 37,239 (identifying "managing related reserves . . .. or providing custodial services for reserve assets" and "providing custodial or safekeeping services for payment stablecoins, required reserves, or private keys of payment stablecoins" as activities that may establish a formal relationship under the "account" definition).

[26] *See* NPRM at 37,239 (explaining that the proposed definitions are "designed to clarify that a PPSI's CIP obligation extends to direct relationships . . . and does not extend to activity where the only interaction is with a PPSI's smart contract").

centralization and privacy risks discussed below, which should be addressed in any system allowing for digital identity solutions.

A. Digital Identity Solutions Should Follow a Technology-Neutral Framework

Digital identity solutions and verifiable credentials should be explicitly acknowledged in the regulatory text as permissible non-documentary verification methods, without prescribing, entrenching, or mandating any particular technical method, standard, or system of digital identity verification for PPSIs (Question 5).

The NPRM acknowledges "the interest in leveraging verifiable credentials and digital identity as part of account opening procedures," and notes that "a digital identity credential offered by a non-governmental entity that enables a person to prove that they are who they claim to be without revealing information other than that fact could, if appropriate as part of a risk-based procedure, be a non-documentary verification method."[27]

The NPRM also observes that "FinCEN and the Agencies expect that PPSIs would treat different digital identity tools differently," and that "technological variation and innovation are best accounted for by maintaining the flexibility in the proposal relating to how a PPSI verifies a customer's identity."[28] The final rule should preserve that flexibility: different technical mechanisms for identity verification should be permitted based on whether they achieve reliable customer identification, not on their precise technological form.

For these reasons, the regulatory text should acknowledge digital identity solutions and verifiable credentials as permissible non-documentary verification methods under § 1033.220(a)(2)(ii)(B), subject to the PPSI's risk-based assessment of the trustworthiness and reliability of the specific tool. This approach would provide regulatory certainty for PPSIs that wish to leverage these tools and would encourage innovation in identity verification, without locking in any particular solution or creating new honeypots of sensitive personal information.

FinCEN and the Agencies should also clarify that digital identity solutions that enable a person to prove their identity without revealing unnecessary personal information, including zero-knowledge proof systems and privacy-preserving verifiable credentials, may qualify as permissible non-documentary verification methods, provided they enable the PPSI to form a reasonable belief that it knows the true identity of the customer. Consistent with our prior submissions urging regulators to avoid mandating any single technical architecture for sanctions compliance,[29] the same principle should govern identity verification here.

[27] NPRM at 37,242.
[28] NPRM at 37,242.
[29] *See* Nov. 2025 Comment Letter at 5.

B. Digital Identity Solutions Should Be Evaluated Within a Risk-Based Framework to Protect User Information.

Digital identity solutions and verifiable credentials offer meaningful advantages over traditional identity verification methods, but their use should be governed by a risk-based framework that evaluates tools based on functional outcomes rather than technological form — given the significant risks they present, particularly the creation of honeypots of sensitive personal information (Question 6).

The risks associated with digital identity solutions counsel against mandating their use for CIP purposes. In particular:

- **Creation of information honeypots:** The most significant risk associated with digital identity solutions is the creation of concentrated repositories of sensitive personal information, posing risks to both individual users and U.S. national security.[30] A digital identity issuer must collect PII — specifically credentials such as government-issued IDs — to issue verifiable credentials. Since U.S. policy generally requires financial institutions and government entities to retain the PII they collect, the risks associated with centralized data collection remain.[31] This is not a theoretical concern: PII was the most stolen data source globally in 2024, and major financial institutions have experienced large-scale data breaches compromising the sensitive personal information of 100 million Americans.[32] The final rule should not mandate digital identity solutions in a manner that creates new centralized repositories of sensitive personal information.

- **Varying reliability and trustworthiness:** Digital identity tools vary significantly in how they operate and in their trustworthiness, and the methods used to authenticate identity for issuing verifiable credentials themselves present risks of fraud and discrimination. Confirmation code verification is vulnerable to phishing, stolen devices, and interception attacks; facial and biometric comparison are becoming less reliable as AI-generated synthetic media grows more sophisticated; and device or account tenure checks can be discriminatory to certain groups, including immigrants or young adults who have recently acquired a device or account.[33] Given this variation, PPSIs must carefully assess the reliability and security of any digital identity solution before relying on it for CIP purposes, and FinCEN and the Agencies should address this risk through a risk-based

[30] Oct. 2025 RFI Response at 7.
[31] The requirement for credential-issuers to retain PII means that privacy risks still remain, even if digital identity solution systems adopt zero-knowledge proofs. Zero-knowledge proof systems represent an important innovation that provides significant privacy protections, enabling a person to prove the validity of information without revealing the information itself. *See generally, .Oct. 2025 RFI Response* at 11-13.
[32] *See* Oct. 2025 RFI Response at 4 (discussing the 2019 Capital One data breach, which exposed names, Social Security numbers, addresses, account numbers, and other sensitive personal information).
[33] Oct. 2025 RFI Response at 10-11.

framework rather than through prescriptive requirements mandating specific tools or architectures.

- **Risk of premature standardization:** Mandating specific digital identity standards or architectures in the regulatory text, whether directly or through the uncertainty created by an unaddressed regulatory gap, would risk entrenching today's tools before more effective, privacy-preserving alternatives can emerge. The final rule should instead explicitly acknowledge digital identity solutions as permissible verification methods while maintaining the technology-neutral framework needed for innovation. Rather than dictating architecture, FinCEN and the Agencies should support the safe, privacy-respecting development of this technology in partnership with the private sector, leaving developers free to innovate improved solutions.

FinCEN and the Agencies could also address these risks in guidance rather than entrenching prescriptive regulatory requirements, consistent with the technology-neutral, principles-based approach reflected in the proposed rule and in our prior submissions.

VI. Targeted Clarifications Would Support Innovation Without Increasing Illicit Finance Risk

Several targeted clarifications would make the proposed rule more conducive to industry innovation while maintaining robust CIP compliance and protecting against illicit finance risk (Question 8).

As discussed above, an unambiguous affirmation of the treatment of secondary market activity and a technology-neutral, risk-based approach to identity verification would each reduce compliance burdens and provide PPSIs with regulatory certainty. Neither change would increase illicit finance risk, since PPSIs would remain independently subject to risk-based assessment obligations. FinCEN and the Agencies should also preserve a practical implementation timeline, extending the same regulatory certainty to the compliance process itself. At a minimum, the proposed 12-month effective date should remain in place, with phased implementation or supervisory flexibility available for technical capabilities that require smart contract upgrades, multi-chain deployment planning, or third-party audits. A workable timeline supports compliance without encouraging the kind of rushed deployment that could introduce the very security vulnerabilities or compliance gaps the rule is designed to prevent.

* * *

DEF and SPI appreciate the opportunity to comment and welcome further engagement as the rulemaking proceeds.

Respectfully submitted,

On behalf of DEF,

Amanda Tuminelli
CEO & CLO

On behalf of SPI,

Patrick Wilson
General Counsel