Transparency International U.S.
1100 13th St NW
Suite 800
Washington, DC 20005
Tel: +1 (202) 642-1515
info-us@transparency.org
us.transparency.org

August 21, 2026

Financial Crimes Enforcement Network
Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration

Re: Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37234

To the Agencies:

Transparency International U.S. (TI US) appreciates the opportunity to comment on the joint proposed rule implementing the customer identification program (CIP) requirements of the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act.

TI US is part of the world's largest global coalition dedicated to fighting corruption. With more than 100 national chapters worldwide, Transparency International (TI) works with citizens, governments, and the private sector to promote transparency and accountability, strengthen the rule of law, and curb the abuse of power in all its forms.

We support the proposed rule's general approach that permitted payment stablecoin issuers (PPSIs) should be required to know who their direct customers are. Yet the final rule should make sure that "know your customer" means more than just collecting four identifying fields and confirming that a company exists.[1]

This comment builds on our November 2025 comment on the implementation of the GENIUS Act, and our June 2026 comment on the related AML/CFT and sanctions rule for PPSIs. Across those comments, our point has been consistent: Stablecoin regulation should be risk-based, workable, and focused on the places where dirty money can actually enter and move through the U.S. financial system.[2]

Overview

The Agencies are right to treat CIP as part of a PPSI's broader AML/CFT program, as opposed to some stand-alone paperwork exercise. Stablecoins are dollar-linked, fast-moving, global, and easily transferred across wallets and platforms. Those features certainly make them useful to legitimate users, but they also make them useful to criminals trying to move or hide the proceeds of corruption, fraud, drug and human trafficking, sanctions evasion, and other crimes.

The body of evidence illustrating such risks is only growing. For example, a 2023 Transparency International Anti-Corruption Helpdesk report found that criminals can exploit cryptocurrencies'

---

[1] Financial Crimes Enforcement Network, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and National Credit Union Administration, "Permitted Payment Stablecoin Issuer Customer Identification Program," 91 Fed. Reg. 37234, June 22, 2026.

[2] TI US, "Comment on FinCEN's Proposed Rule for Stablecoin Issuers under the GENIUS Act," June 9, 2026, https://us.transparency.org/resource/comment-on-fincens-proposed-rule-for-stablecoin-issuers-under-the-genius-act/; TI US, "TI US Comment on Implementation of the GENIUS Act," Nov. 4, 2025, https://us.transparency.org/resource/ti-us-comment-on-implementation-of-the-genius-act/.

pseudonymity, global reach, and regulatory gaps to facilitate money laundering, corruption, sanctions evasion, and other illicit activity.[3] This past May, the Financial Crimes Enforcement Network (FinCEN) issued an alert regarding the Islamic Revolutionary Guard Corps' (IRGC) use of shell companies, financial facilitators, and digital assets as a means of moving and laundering state-linked illicit proceeds.[4] And the U.S. Department of Justice has alleged that a U.S.-based crypto payment company moved more than $500 million in overseas payments while concealing the source and purpose of transactions and failing to maintain an effective anti-money laundering (AML) program.[5]

The throughline here is simple: Identity information is most useful when it helps connect a customer to the entities, wallets, intermediaries, and transactions that create illicit finance risk. The proposed rule gets that essential foundation right, but several targeted changes would make the CIP significantly more useful to the financial institutions that have to assess customer risk and, downstream, to law enforcement and regulators trying to trace illicit activity.

I. The risk assessment should expressly include corruption, political exposure, and opaque ownership.

Concern: Proposed § 1033.220(a)(2) requires risk-based identity verification, and directs PPSIs to consider account type, account-opening method, available identifying information, and the issuer's size, location, and customer base. Those are reasonable factors, but they do not expressly identify the illicit finance risks that should drive enhanced verification. For a stablecoin issuer, risk can rise sharply when a customer is a foreign political figure, state-linked entity, anonymous or otherwise opaque company, nominee, intermediary, or person tied to a high corruption- or sanctions-risk jurisdiction.[6]

Suggested change: The Agencies should add the following sentence to proposed § 1033.220(a)(2):

> The assessment shall include, where relevant, risks involving corruption, bribery, embezzlement of public funds, kleptocracy, sanctions evasion, foreign political figures and their close associates, state-owned or state-linked enterprises, anonymous or otherwise opaque legal entities, nominee or intermediary arrangements, high-risk jurisdictions, and other illicit finance indicators identified by FinCEN.

II. A PPSI should connect a direct customer's identity to the wallets used in that relationship.

Concern: Proposed § 1033.220(a)(2)(i) requires a customer's name, date of birth or formation, address, and identification number. That makes sense for ordinary identity verification, but stablecoin activity happens through blockchain addresses. A PPSI can know that, say, ABC Trading Ltd. exists, while still

---

[3] Transparency International Anti-Corruption Helpdesk, "Cryptocurrencies, Corruption and Organised Crime: Implications of the Growing Use of Cryptocurrencies in Enabling Illicit Finance and Corruption," Mar. 28, 2023, https://knowledgehub.transparency.org/helpdesk/cryptocurrencies-corruption-and-organised-crime-implications-of-the-growing-use-of-cryptocurrencies-in-enabling-illicit-finance-and-corruption.

[4] FinCEN, "FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds," FIN-2026-Alert002, May 11, 2026, https://www.fincen.gov/news/news-releases/fincen-issues-alert-stop-money-laundering-iranian-revolutionary-guard-corps.

[5] U.S. Department of Justice, "Founder of Cryptocurrency Payment Company Charged with Evading Sanctions and Export Controls," June 9, 2025, https://www.justice.gov/opa/pr/founder-cryptocurrency-payment-company-charged-evading-sanctions-and-export-controls.

[6] 91 Fed. Reg. at 37271; proposed 31 C.F.R. § 1033.220(a)(2).

failing to connect ABC to the wallets it uses to receive newly issued tokens, redeem them, or interact directly with the issuer. As we explained in our June comment, a stablecoin issuer that knows a customer's legal name, but not the wallets used in the customer relationship, has only half a compliance picture.

Suggested change: Add a new § 1033.220(a)(2)(i)(A)(5) that reads:

> For a customer that uses a distributed-ledger address or other digital asset identifier in connection with the account, each such address or identifier provided to, used with, or otherwise known by the permitted payment stablecoin issuer, together with risk-based procedures reasonably designed to keep that information current.

This wouldn't require an issuer to identify every person who later receives or uses its stablecoin; it would just require the issuer to keep track of the digital wallet addresses its own customers use when dealing with the issuer. If a customer provides a wallet address to receive newly issued stablecoins or to redeem stablecoins for dollars, the issuer should record that the customer is using that wallet.

III. Verifying a legal entity's existence is only the first step.

Concern: Under the proposed rule, a PPSI would begin by collecting basic identifying information about a legal entity customer, such as its name, address, formation date, and identification number. It would then verify that information using corporate records or other documents. If those methods are enough to verify the legal entity's identifying information, the CIP does not require the PPSI to obtain information about the people who control the account. It's only when the PPSI cannot verify the legal entity through documentary or non-documentary methods that the proposed rule would require it to obtain information about individuals with authority or control over the account.

But this requirement is too narrow: Anonymous companies, trusts, nominees, and layered ownership structures are basic tools for hiding corruption proceeds. A certificate of incorporation may prove that a company exists, but it does not tell the issuer *who* is directing the relationship or why the relationship may present elevated risk.[7]

Suggested change: Replace the limiting second sentence of proposed § 1033.220(a)(2)(ii)(C) with:

> For a customer that is not an individual, the customer identification program shall include risk-based procedures to obtain and, as appropriate, verify information concerning individuals who exercise authority or control over the account and, where required by applicable customer due diligence requirements or warranted by heightened risk, individuals who directly or indirectly own or control the customer. These procedures apply whether or not the issuer can verify the legal existence of the customer through documentary or non-documentary means.

Importantly, this change wouldn't turn CIP into a second beneficial ownership rule. It would just make clear that legal existence and identity risk are not the same question (because they are not). This approach is consistent with our broader recommendation that incomplete or opaque ownership information should itself be treated as a risk factor rather than as a reason to simply stop asking questions.[8]

IV. The secondary-market exclusion must contain an anti-evasion rule.

---

[7] 91 Fed. Reg. at 37271; proposed 31 C.F.R. § 1033.220(a)(2)(ii)(C).

[8] TI US, "Comment on FinCEN's Proposed AML/CFT Program Rule," June 9, 2026, at 3, https://us.transparency.org/resource/comment-on-fincens-proposed-aml-cft-program-rule/.

Concern: Proposed § 1033.100(b)(2)(iv) excludes from the definition of "customer" anyone who buys or redeems a stablecoin through an intermediary rather than directly with the issuer. We don't recommend requiring PPSIs to run CIP on every secondary-market holder. But at the same time, a direct customer shouldn't be able to evade CIP by acting as an undisclosed nominee, conduit, or intermediary for someone else.[9]

Suggested change: Add the following sentence, or language with the same operative effect, to proposed § 1033.100(b)(2)(iv):

> The exclusion does not apply if the issuer knows or suspects that a direct customer is opening, maintaining, or using the account on behalf of another person as an undisclosed agent, nominee, intermediary, or conduit.

V. Higher-risk reliance arrangements should require more than an annual certification.

Concern: Proposed § 1033.220(a)(6) allows a PPSI to rely on another regulated financial institution's CIP where the reliance is reasonable and the institution annually certifies that it has implemented its anti-money laundering/countering the financing of terrorism (AML/CFT) program and will perform specified CIP requirements.[10] This may be enough for ordinary, low-risk relationships, but where the relied-upon institution handles high volumes, has substantial exposure to foreign or nested services, or serves elevated-risk customers, reasonable reliance plus an annual certification may still provide too little assurance that the required customer verification is being performed effectively.

Suggested change: Add the following to proposed § 1033.220(a)(6)(i):

> Reliance is reasonable under the circumstances only where the permitted payment stablecoin issuer has taken risk-based steps appropriate to the relationship to assess the relied-upon financial institution's customer-identification controls, can obtain relevant underlying identification information when reasonably necessary for compliance or law enforcement purposes, and is not aware of material deficiencies in that institution's AML/CFT or customer-identification controls.

VI. Unverified high-risk customers should not be allowed to transact freely while verification is pending.

Concern: Proposed § 1033.220(a)(2)(iii) rightly requires a PPSI to decide when an account should not be opened, when it should be closed, and the terms under which a customer may use an account while identity verification is still underway. The final rule should make clear that this flexibility is not a temporary safe harbor for customers presenting obvious illicit finance risks.[11]

Suggested change: Revise proposed § 1033.220(a)(2)(iii)(B) to state:

> The permitted payment stablecoin issuer must establish the terms under which a customer may use an account while the issuer attempts to verify the customer's identity, including appropriate restrictions on transactions, issuance, redemption, custody, or transfers. A permitted payment stablecoin issuer shall not permit unrestricted use of an account where identity verification remains incomplete and the issuer has identified heightened money

---

[9] 91 Fed. Reg. at 37270; proposed 31 C.F.R. § 1033.100(b)(2)(iv).
[10] 91 Fed. Reg. at 37272; proposed 31 C.F.R. § 1033.220(a)(6).
[11] 91 Fed. Reg. at 37271; proposed 31 C.F.R. § 1033.220(a)(2)(iii).

laundering, terrorist financing, sanctions, corruption, fraud, trafficking, or other illicit finance risk.

Conclusion

The final rule does not need to require PPSIs to identify every person who ever touches a stablecoin. But it should ensure that issuers assess the illicit finance risks that matter, connect direct customers to the wallets they use, look beyond a legal entity's formation documents when risk warrants identifying the people controlling the relationship, prevent customers from evading CIP through undisclosed intermediaries, take appropriate, risk-based steps when relying on another institution's customer identification, and restrict activity where identity verification remains incomplete and illicit finance risk is elevated.

Those changes would preserve the proposal's workable boundaries while making CIP fit the product it regulates. They would also keep the rule consistent with the broader GENIUS implementation framework, that financial activity should carry financial crime safeguards that match the actual risk, and formal distinctions should not create new places for dirty money to hide.

Thank you for the opportunity to comment on this rulemaking. For additional information or questions, please contact Scott Greytak, Deputy Executive Director of Transparency International U.S., at sgreytak@us.transparency.org.

Respectfully submitted,

Scott Greytak
Deputy Executive Director

Gary Kalman
Executive Director