TRANSPARENCY INTERNATIONAL U.S.
fighting corruption, promoting democracy

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

June 9, 2026

U.S. Department of the Treasury
Regulatory and Strategic Affairs Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: Comment on Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, Docket No. FINCEN-2026-0100; RIN 1506-AB73

Dear Director Gacki:

Transparency International U.S. (TI US) appreciates the opportunity to comment on the proposed rule implementing anti-money laundering, countering the financing of terrorism, and sanctions compliance requirements for permitted payment stablecoin issuers under the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act.[1]

We strongly urge the U.S. Department of the Treasury (Treasury) to fully implement key provisions of the Act in order to close illicit finance gaps and strengthen U.S. leadership on global anti-money laundering and countering the financing of terrorism (AML/CFT) standards. Building on our prior recommendations to U.S. Senate leadership during negotiations on the GENIUS Act,[2] as well as our comment in response to the Advance Notice of Proposed Rulemaking (ANPRM),[3] we offer the following in support of a strong and effective implementation process that upholds U.S. commitments to transparency, accountability, and financial integrity.

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.

Overview

TI US supports the thrust of Treasury's efforts here, that stablecoin issuers should not sit outside the Bank Secrecy Act (BSA). But this rule must do more than check a box. If stablecoins are going to become a bigger

---

[1] Financial Crimes Enforcement Network, "Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements," 91 Fed. Reg. 18582, 18582-18667, Apr. 10, 2026, https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.

[2] TI US, Free Russia Foundation, Financial Accountability and Corporate Transparency (FACT) Coalition, and Nate Sibley, Kleptocracy Initiative, Hudson Institute, "Urgent Amendments Needed to Address Illicit Finance Risks in the GENIUS Act," May 7, 2025, https://us.transparency.org/resource/letter-from-counter-kleptocracy-groups-urging-amendments-to-the-genius-act/.

[3] 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/.

part of the financial system, the safeguards that apply to them need to be built for the risks that we know are already here.

Stablecoins are no longer a niche product. They are becoming one of the central settlement tools of the digital asset economy. They are dollar-linked, fast-moving, global, programmable, and accessible across borders. Those features are what makes them attractive to legitimate users, yet also to corrupt officials, sanctions evaders, scammers, traffickers, ransomware actors, cartel-linked networks, and authoritarian regimes looking for a way around the formal banking system.

Treasury recognizes this. The proposed rule itself notes that the U.S. government has linked stablecoins to scammers and fraudsters; Democratic People's Republic of Korea (DPRK) information technology workers, who use false identities and remote work schemes to generate revenue for the North Korean regime and evade sanctions; cybercriminal groups and related money laundering networks; drug traffickers; terrorist groups; and sanctions evasion and money laundering networks.[4]

Outside data raises additional concerns. For example, Chainalysis reported that **stablecoins accounted for 84 percent of all illicit crypto transaction volume in 2025**, noting that illicit actors use stablecoins for many of the same reasons that legitimate users do (cross-border transferability, lower volatility, and broader utility).[5] TRM Labs similarly reported that illicit crypto volume reached $158 billion in 2025 (an all-time high), with Russia-linked flows driving significant sanctions evasion and Chinese-language escrow and money laundering networks processing more than $100 billion.[6]

The associated corruption risk is not abstract. Stablecoins can be used to move bribe payments, embezzled funds, procurement kickbacks, sanctions-evasion payments, and stolen state assets with fewer chokepoints than the traditional banking system. They can also support financial networks that keep corrupt and authoritarian regimes alive. For instance, Reuters has reported that Russia used cryptocurrency in oil trade with China and India to skirt Western sanctions,[7] and that U.S. lawmakers pressed the Biden Administration on the use of crypto, including the stablecoin Tether, by sanctioned entities in Russia, Iran, and North Korea.[8] More recently, the same outlet reported that the United Kingdom sanctioned Russia-linked crypto networks described as shadow financial systems supporting Russia's war economy.[9]

Iran presents another warning sign, as the proposed rule notes that Iranian actors and other sanctioned parties have used stablecoins and other digital assets to evade restrictions and move value outside the formal banking

---

[4] Financial Crimes Enforcement Network, "Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements," 91 Fed. Reg. 18582, 18586 & nn.48-52, Apr. 10, 2026, https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.

[5] Chainalysis Team, "2026 Crypto Crime Report Introduction," Chainalysis, Jan. 8, 2026, https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.

[6] TRM Labs, "2026 Crypto Crime Report," Jan. 28, 2026, https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report; TRM Labs, "Stablecoins at Scale," Feb. 17, 2026, https://www.trmlabs.com/resources/blog/stablecoins-at-scale-broad-adoption-and-highly-concentrated-illicit-networks.

[7] Reuters, "Russia leans on cryptocurrencies for oil trade, sources say," Mar. 14, 2025, https://www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/.

[8] Reuters, "U.S. lawmakers press Biden administration on use of crypto to evade sanctions," Apr. 29, 2024, https://www.reuters.com/world/us/us-lawmakers-press-biden-administration-use-crypto-evade-sanctions-2024-04-29/.

[9] Reuters, "UK targets Russian crypto networks in latest sanctions," May 26, 2026, https://www.reuters.com/world/uk-targets-russian-crypto-networks-latest-sanctions-2026-05-26/.

system.[10] North Korea presents a different but related threat, with Treasury noting DPRK-linked cybercriminal activity involving stablecoins and related laundering networks,[11] while outside reporting and blockchain analysis have documented billions in stolen cryptocurrency tied to DPRK actors[12] and weapons-proliferation financing.[13]

Despite the occasionally dense and technical rhetoric that accompanies stablecoins and other digital assets, the throughline here is rather simple: If stablecoins are going to become a major way that dollar-denominated payments move, then those who issue them cannot pretend that they stand off to the side, running neutral software. They are now key gatekeepers to a new financial system. If you can mint the asset, redeem it, freeze it, blacklist wallets, and monitor what is happening across the network, you are not a bystander. You are part of the control architecture, and the rules should treat you that way.

Treasury must strengthen its proposed rule to reflect this reality. In particular:

I. The final rule should require ecosystem-wide monitoring, not just narrow primary-market compliance.

Concern: The proposed rule recognizes that most stablecoin issuers interact directly with a small number of institutional participants, and that those institutions then distribute stablecoins into broader circulation. The proposal also recognizes that issuers often use smart contracts that allow them to prohibit specific wallet addresses from interacting with the stablecoin. In plain English, issuers may not know every end user, but they often have visibility and control that matters. If the rule focuses too narrowly on issuance and redemption, it will miss much of the actual risk.

Needed changes: FinCEN should require each permitted payment stablecoin issuer (PPSI) to monitor risk across the full lifecycle of its stablecoin, not only at issuance and redemption. That should include activity the issuer can see or reasonably identify through blockchain analytics, wallet-risk data, sanctions screening, available customer and counterparty information, law enforcement requests, and other available tools.

II. The final rule should not create a smart-contract loophole for suspicious activity reporting.

Concern: Proposed 31 CFR 1033.320(g) would state that a transaction is not conducted or attempted by, at, or through a permitted payment stablecoin issuer only because a third-party transfer *results* in an interaction with the issuer's smart contract. That language may be intended to prevent limitless suspicious activity reporting (SAR) liability for every on-chain transfer, but written too broadly, it risks becoming the rule's escape hatch. Criminals do not care whether a transfer is called a customer transaction, a secondary-market transfer, or a smart-contract interaction. They care whether the money moves.

---

[10] Reuters, "Iran's surging crypto activity draws U.S. scrutiny," Feb. 3, 2026, https://www.reuters.com/business/finance/irans-surging-crypto-activity-draws-us-scrutiny-2026-02-03/.
[11] Financial Crimes Enforcement Network, "Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements," 91 Fed. Reg. 18582, 18586 & n.49, Apr. 10, 2026, https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.
[12] Chainalysis Team, "2025 Crypto Theft Reaches $3.4 Billion," Chainalysis, Dec. 18, 2025, https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/.
[13] Reuters, "'It's scary' - crypto workers under siege from North Korean hackers," Sept. 4, 2025, https://www.reuters.com/world/asia-pacific/its-scary-crypto-workers-under-siege-north-korean-hackers-2025-09-04/.

Needed changes: FinCEN should revise proposed 31 CFR 1033.320(g) to make clear that this limitation does not apply where the issuer knows, suspects, has reason to suspect, or has reasonably available information indicating that a transaction or pattern of transactions involves illicit finance, sanctions evasion, corruption proceeds/financing, fraud, trafficking, ransomware, or other criminal activity. The final rule should also state that a permitted payment stablecoin issuer (PPSI) must file a SAR when suspicious secondary-market activity is visible to the issuer, detected through its monitoring systems, connected to its customer or counterparty relationships, tied to a blocked or high-risk wallet, reflected in on-chain flows involving its stablecoin, or otherwise within the issuer's compliance capability.

III. The SAR threshold should remain at $2,000 for PPSIs—or at least for secondary-market and high-risk activity.

Concern: FinCEN proposes a $5,000 SAR threshold for PPSIs, even though stablecoin issuers regulated as money services businesses (MSBs) currently have a $2,000 threshold. FinCEN explains that primary-market transactions below $5,000 may be rare. That may be true for some direct issuer relationships, but it does not answer the real illicit finance problem: Corrupt actors, scammers, sanctions evaders, and laundering networks can structure activity, use multiple wallets, move funds through intermediaries, and break activity into smaller pieces.

Needed changes: FinCEN should apply a $2,000 SAR threshold to PPSIs as well. If FinCEN declines to do that across the board, it should at least apply a $2,000 threshold to secondary-market activity, activity involving high-risk jurisdictions, mixers, nested services, darknet markets, sanctioned or previously sanctioned platforms, high-risk exchanges, corruption-related typologies, foreign political figures, and activity involving suspected structuring. The final rule should also make clear that issuers cannot treat connected activity as isolated transactions. If multiple wallets, accounts, funding sources, or transaction patterns point to the same person or network, issuers should be required to look at that activity together.

IV. Customer due diligence must look beyond the customer's name.

Concern: FinCEN considered, but did not propose, requiring PPSIs to collect additional information such as customers' blockchain wallet addresses and other risk-relevant information. That is insufficient. A stablecoin issuer that knows a customer's legal name but not the wallets that customer uses has only half a compliance program.

Needed changes: FinCEN should require PPSIs, at onboarding and on an ongoing basis, to collect and verify wallet addresses used by direct customers for issuance, redemption, custody, transfer, or other PPSI-related activity, and to require customers to update that information. For legal entity customers, FinCEN should require PPSIs to collect risk-based information sufficient to understand the customer's business model, source of funds, expected stablecoin activity, and associated wallets. PPSIs should also be required to screen customer-linked wallets for exposure to sanctions, mixers, illicit services, high-risk exchanges, ransomware, scams, darknet markets, trafficking networks, corruption-related typologies, and other red flags.

V. Offshore platforms should not become an easy way around U.S. anti-money laundering rules.

Concern: Treasury notes that stablecoin issuers often issue stablecoins to a small number of larger companies, including digital asset exchanges, which then put the stablecoins into broader circulation. That structure creates a major risk, though, because a PPSI can be "clean" at the front door while its product is pushed through offshore exchanges, nested services, and weakly regulated intermediaries that serve corrupt officials and other criminals.

Needed change: FinCEN should require stablecoin issuers to know who is moving large volumes of their coins, especially through foreign exchanges, offshore platforms, distributors, and other major partners. That

means knowing who owns or controls those partners, where they operate, whether they are licensed, whether they have real anti-money laundering controls, and whether they can respond to law enforcement when something goes wrong. The rule should be simple: if a major partner will not provide basic transparency, the issuer should not be allowed to keep doing business with it.

VI. Stablecoin rules must account for corrupt officials and their networks.

Concern: The proposed rule would apply special standards of diligence for correspondent and private banking accounts, including private banking accounts for senior foreign political figures. That is essential, but the rule should go farther by speaking openly about corruption risk. Stablecoins can move the proceeds of bribery, embezzlement, procurement fraud, sanctions evasion, kleptocracy, and state capture, so a program that treats corruption as an afterthought will miss one of the most important reasons bad actors want and use these tools.

Needed change: FinCEN should require PPSIs to address corruption risk expressly in their AML/CFT programs, risk assessments, customer due diligence, enhanced due diligence, monitoring, SARs processes, and training. The final rule should require enhanced due diligence for senior foreign political figures, their family members, close associates, state-owned enterprise officials, high-risk public procurement actors, and legal entities owned or controlled by such persons. That review should look at where the person's money came from, an entity's beneficial ownership information, whether high-risk jurisdictions or sanctioned actors are involved, and whether the customer's wallets show signs of suspicious or illicit activity.

VII. Issuers should be required to stop illicit stablecoin activity when they have the power to do so.

Concern: Treasury correctly recognizes that many stablecoin smart contracts allow issuers to prohibit specific wallet addresses from transferring, redeeming, or moving stablecoins. But the rule should not leave too much discretion around whether issuers build and maintain technical controls. If a stablecoin issuer can freeze illicit value but chooses not to build the systems to do so quickly and reliably, the result is predictable, as criminals will simply move faster than compliance teams.

Needed change: Treasury's Office of Foreign Assets Control (OFAC) and FinCEN should require PPSIs to maintain technical capabilities, where technically feasible, to identify, block, freeze, reject, and, where lawful and appropriate, prevent further movement of stablecoins connected to sanctions, lawful orders, or high-confidence indicators of sanctions exposure or illicit finance risk. The final rule should require issuers to document these capabilities, test them regularly, maintain escalation procedures, and report failures or material delays to the appropriate regulator. If an issuer claims it cannot build or use these controls, it should have to explain why and get approval from its regulator.

VIII. Stablecoin issuers should not be allowed to promise cooperation with law enforcement unless they can actually deliver it.

Concern: It is not enough for the rule to say that issuers must comply with lawful orders. Issuers must instead have the people, systems, records, and tools needed to identify suspicious wallets, escalate urgent requests, freeze funds when legally required, and preserve evidence. Stablecoins can move across wallets and exchanges very quickly. If an issuer cannot respond just as timely, compliance may come too late to matter.

Needed changes: FinCEN and OFAC should require stablecoin issuers to have an actual plan for responding to lawful orders. This means knowing who is "on call", how urgent requests are to be escalated, how suspicious wallets are checked, how funds can be frozen when legally required, how records are preserved, when regulators are notified, and how the issuer will coordinate with law enforcement. Those plans should not just exist on paper: Issuers should be required to test them at least once a year and whenever they make major changes to their systems.

IX. Recordkeeping and Travel Rule obligations should be tailored to stablecoins and codified in Part 1033.

Concern: FinCEN asks whether recordkeeping and Travel Rule obligations would be clearer if it codified a PPSI-specific rule in Part 1033. The answer is yes. Stablecoins do not fit neatly into traditional categories written for bank wires and money transmission. If FinCEN leaves too much ambiguity, issuers and intermediaries will exploit the gray areas and law enforcement and victims of crime will inevitably pay the price.

Needed changes: Issuers should be required to keep and provide the basic information needed to trace illicit stablecoin activity. That includes the wallets involved, the transactions at issue, the customers and counterparties connected to them, and any information the issuer has linking those wallets to real people or companies. FinCEN should also make clear that these obligations apply to stablecoins because they are used to move and store value.

X. Information sharing should be made practical and expected, not just voluntary.

Concern: FinCEN asks whether stablecoin issuers would participate in voluntary information sharing under Section 314(b). They should, but that should not be treated as some box-checking compliance option. Illicit activity can move quickly across exchanges, wallets, chains, and issuers. No single company sees the whole scheme, which is exactly why information sharing is important.

Needed changes: FinCEN should make clear that a reasonably designed PPSI AML/CFT program should include policies and procedures for participation in 314(b) information sharing where appropriate. FinCEN should also develop stablecoin-specific typology guidance for such sharing, including with regards to corruption proceeds/financing.

XI. Certifications should be signed by senior officers and backed by personal accountability.

Concern: The proposal requires AML/CFT program certification, and OFAC would require PPSIs to provide sanctions program certifications upon request. We welcome this requirement, but certification can become a paperwork exercise unless the signer has real responsibility and the agency has enough information to test that certification.

Needed changes: FinCEN and OFAC should require senior leaders at stablecoin issuers to certify annually that the company has a reasonably designed, risk-based, and effective program to prevent money laundering, sanctions evasion, and other illicit finance. That certification should be signed by the CEO, the chief compliance officer, and a senior official responsible for the issuer's product or technology systems. Those officials should have to confirm that the issuer has working controls to monitor suspicious activity, screen risky wallets and partners, respond to lawful orders, and freeze or block funds when legally required. The certification should also be approved by the board and supported by records that regulators can review.

XII. The core pieces of the final rule should take effect much sooner.

Concern: FinCEN proposes giving stablecoin issuers 12 months after the finalization of the rule to comply. But the risks are already here, and a full year before basic AML and sanctions safeguards apply would leave a dangerous gap and could invite a rush of risky activity before the rules come online.

Needed change: FinCEN and OFAC should require the core obligations to take effect within 180 days. That should include AML programs, sanctions screening, customer due diligence, suspicious activity reporting, lawful-order response, and procedures to freeze or block funds when legally required and technically feasible.

FinCEN can allow more time for complex technology changes, but only when an issuer explains what it needs to build, sets a clear timeline, and maintains interim safeguards while that work is underway.

Conclusion
Treasury must bring PPSIs into the AML/CFT and sanctions compliance frameworks, but the final rule must match the risks we are already seeing. Stablecoins are not just a new consumer payment tool. They are becoming a global dollar–equivalent payment rail that can be exploited by drug cartels, human traffickers, scammers, sanctioned regimes, cybercriminals, and corrupt officials. The final rule should not pretend that the only meaningful risk occurs when an issuer mints or redeems a token. It should reflect the reality that risk follows the stablecoin wherever it moves.

At bottom, **if stablecoins are going to benefit from the credibility of the U.S. dollar, they must also carry the basic safeguards that protect the U.S. financial system from corruption and other crimes.**

We urge Treasury to pursue robust implementation of the GENIUS Act consistent with the above recommendations. A well-implemented framework can support responsible innovation while preventing the kinds of corruption and financial crime that erode trust in financial systems around the world.

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
Transparency International U.S.

Gary Kalman
Executive Director
Transparency International U.S.