

October 8, 2026

Jenna Casanova
Acting Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
P.O. Box 39
Vienna, VA 22183

Re: Preserving and strengthening digital asset anti-money laundering safeguards

Dear Acting Director Casanova:

Transparency International U.S. (TI US) urges the Financial Crimes Enforcement Network (FinCEN) to promptly advance tailored safeguards addressing international convertible virtual currency mixing and unhosted wallet transactions, following its withdrawal of two proposed rules intended to address these risks.¹ Neither proposal had taken effect, so the withdrawals do not repeal existing requirements. But they leave high-risk information gaps unresolved, with no replacement safeguards in place. Those gaps make it easier for corrupt officials to hide bribe payments, transfer money stolen from the public, and move illicit funds through the United States and around the world. The withdrawals are a setback for efforts to combat money laundering and illicit finance, regardless of the fate of the CLARITY Act, which itself falls short of addressing significant vulnerabilities in the digital asset ecosystem. **FinCEN has the authority to address these risks now—abandoning efforts to close these gaps leaves corrupt officials and other criminals with greater opportunities to exploit them.**

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.²

Our recommendations build on TI US's research and advocacy on the corruption and illicit finance risks of digital assets, including our report, *Crypto's Dirty Money Problem: What Congress Must Fix*,³ and our June 9, 2026 comment on FinCEN's proposed stablecoin anti-money

¹ FinCEN, "FinCEN Announces Withdrawals of Proposed Digital Asset Related Rules," Oct. 5, 2026, <https://www.fincen.gov/news/news-releases/fincen-announces-withdrawals-proposed-digital-asset-related-rules>.

² For more information, see Transparency International, www.transparency.org.

³ TI US, *Crypto's Dirty Money Problem: What Congress Must Fix*, July 13, 2026, <https://us.transparency.org/resource/cryptos-dirty-money-problem-what-congress-must-fix/>.

laundering/countering the financing of terrorism (AML/CFT) requirements under the GENIUS Act.⁴ Throughout this work, we have called for digital asset businesses to identify customers, detect suspicious activity, and give investigators the information they need to trace criminal proceeds. **Stablecoin-specific rules are an important part of that effort, but they cannot substitute for safeguards addressing mixers, unhosted wallet transactions, and other digital asset services.**

FinCEN should use its existing authority under the Bank Secrecy Act (BSA), including its authority to impose special measures under Section 311 of the USA PATRIOT Act, to address the corruption and illicit finance risks of digital assets. Drawing on our research and prior recommendations, we urge the bureau to take the following five actions:

1. Reverse the retreat on international mixing.

FinCEN withdrew both its 2023 proposal and the underlying finding of primary money laundering concern, even while acknowledging that illicit actors continue to use mixers to conceal financial activity and frustrate investigations.⁵ The persistence of this threat demands a stronger regulatory response, not retreat. FinCEN should promptly initiate a new rulemaking to impose targeted requirements under 31 U.S.C. § 5318A, supported by updated findings and the required statutory analysis. The rule should focus on transactions and services that facilitate the concealment of illicit funds, clearly define the required foreign nexus, and require actionable information (including wallet addresses, transaction hashes, amounts, dates, and customer information) while avoiding duplicative reporting. The objective should be straightforward: to deny corrupt officials and other criminals the ability to exploit mixing services to move illicit funds beyond the reach of law enforcement.

2. Close information gaps involving unhosted wallets.

The 2020 proposal sought additional records for covered transactions exceeding \$3,000 and reports for covered transactions exceeding \$10,000, including transactions aggregated under the proposed rule.⁶

The concern involved is hardly new. In 2020, then-Treasury Secretary Steven Mnuchin warned Congress that cryptocurrencies must not become “the equivalent of old Swiss secret number bank accounts.”⁷ His Treasury Department subsequently proposed the very safeguards FinCEN has now withdrawn. Six years later, the risks that prompted those safeguards have not disappeared.

⁴ 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/>.

⁵ FinCEN, “Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern; Withdrawal,” 91 Fed. Reg. 63513, Oct. 6, 2026, <https://www.federalregister.gov/d/2026-20429>.

⁶ U.S. Department of the Treasury, “The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions,” Dec. 18, 2020, <https://home.treasury.gov/news/press-releases/sm1216>.

⁷ Steven T. Mnuchin, Secretary of the Treasury, testimony before the U.S. Senate Committee on Finance, *The President’s Fiscal Year 2021 Budget*, Feb. 12, 2020, <https://www.finance.senate.gov/hearings/the-presidents-fiscal-year-2021-budget>.

FinCEN should establish tailored, risk-based recordkeeping and reporting requirements for transactions between regulated institutions and unhosted wallets. Those requirements should give investigators useful customer and counterparty information, wallet addresses, transaction hashes, amounts, and dates, while avoiding duplicative reporting and ensuring that requirements are proportionate to the risks involved. The requirements should focus on information that regulated institutions can reasonably obtain and verify, with closer scrutiny when corruption or other illicit finance risks are present.

The Prince Group prosecution illustrates the stakes. The U.S. Department of Justice (DOJ) alleges that the Cambodia-based enterprise used trafficked workers to carry out cryptocurrency investment scams, paid bribes to public officials to protect those operations, and laundered proceeds through sophisticated cryptocurrency transactions. More than 127,000 bitcoin associated with the schemes were previously held in unhosted wallets whose private keys were controlled by its chairman.⁸ A wallet address can help investigators follow the money, but they also need to know who controls the wallet.

3. Enforce existing law for offshore and DeFi businesses.

FinCEN's 2019 guidance and Treasury's 2023 decentralized finance (DeFi) risk assessment support enforcing BSA obligations based on what a business actually *does*.⁹ An offshore address or "decentralized" label cannot excuse compliance. Foreign-located money services businesses doing business wholly or substantially within the United States must meet applicable obligations. FinCEN should examine what operators actually do and what they control. Writing software or receiving fees, by itself, should not determine whether BSA obligations apply. And FinCEN should use targeted Section 311 measures against qualifying offshore providers, supported by the requisite findings, while identifying statutory gaps for Congress.

4. Strengthen financial intelligence and support investigators.

FinCEN should clarify that the withdrawals do not alter existing AML program, recordkeeping, Travel Rule, or suspicious activity reporting (SAR) obligations where applicable. Updated guidance should explain relevant corruption, trafficking, fraud, mixing, and cross-chain laundering indicators and the information that makes SARs useful. FinCEN should ensure that institutions preserve and report information connecting suspicious wallet activity to the people behind it. Following the money should lead investigators to the officials who abused their office, and help recover what they stole.

U.S. officials can abuse these same channels. For example, former Drug Enforcement Administration (DEA) agent Carl Mark Force admitted receiving bitcoin for inside law enforcement information and laundering proceeds through transactions designed to conceal their source. Investigators traced the

⁸ DOJ, "Chairman of Prince Group Indicted for Operating Cambodian Forced-Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes," Oct. 14, 2025, <https://www.justice.gov/usao-edny/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged>.

⁹ FinCEN, FIN-2019-G001, May 9, 2019, <https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>; Treasury, "Treasury Releases 2023 DeFi Illicit Finance Risk Assessment," Apr. 6, 2023, <https://home.treasury.gov/news/press-releases/jy1391>.

funds using both blockchain analysis and Silk Road server data.¹⁰ The case demonstrates how financial intelligence and blockchain analysis can expose corruption that might otherwise remain hidden.

5. Complete complementary rules and sustain enforcement capacity.

Finally, FinCEN should finalize and implement strong stablecoin AML/CFT requirements consistent with our June 9, 2026 comment, including secondary-market monitoring and SAR coverage, wallet-linked diligence, offshore partner safeguards, and prompt responses to lawful orders.¹¹ These protections should complement broader digital asset safeguards. In its AML/CFT program rulemaking, FinCEN should require risk assessments to address relevant digital asset vulnerabilities and corruption risks. And the final rule's emphasis on "effectiveness" must preserve accountability for serious compliance failures.¹²

These programs should expressly address bribery, embezzlement, and procurement corruption, including risk-based scrutiny of senior foreign political figures, their family members and close associates, and entities they own or control. As we urged in our GENIUS comment, that scrutiny should consider beneficial ownership, source of funds, and customer-linked wallet activity.

FinCEN also needs the staff and analytical resources to enforce these safeguards. It should identify any additional resources needed and work with Treasury and Congress to secure them. But a lack of new funding should not become an excuse for inaction. FinCEN has tools available now. It should use them. **FinCEN cannot wait for Congress to act while corrupt officials and criminal networks exploit gaps it already has the authority to address.**

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.

¹⁰ DOJ, "Former Silk Road Task Force Agent Sentenced to 78 Months in Prison for Extortion, Money Laundering, and Obstruction," Oct. 19, 2015, <https://www.justice.gov/usao-ndca/pr/former-silk-road-task-force-agent-sentenced-78-months-prison-extortion-money-laundering>.

¹¹ 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/>.

¹² FinCEN, "Fact Sheet: Proposed Rule to Fundamentally Reform Financial Institution AML/CFT Programs," Apr. 7, 2026, <https://www.fincen.gov/system/files/2026-04/Program-NPRM-FactSheet.pdf>.