

July 2025

The Honorable Mike Johnson
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable John Thune
Majority Leader
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Charles E. Schumer
Minority Leader
U.S. Senate
Washington, D.C. 20510

The Honorable Hakeem Jeffries
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

Dear Speaker Johnson, Leader Jeffries, Leader Thune, and Minority Leader Schumer,

As organizations and individuals dedicated to combating kleptocracy, we urge you to amend both the “Guaranteeing Enforceable Necessary Inspections and Uniform Safeguards Act” (GENIUS Act, S.1582) and the “Creating Legal Accountability for Rogue Innovators and Technology Act” (CLARITY Act, H.R. 1167, amendment in the nature of a substitute) before they move forward. As written, both bills would entrench vulnerabilities in digital financial networks—particularly those used by America’s adversaries, corrupt officials, and other bad actors to obscure the financing of sensitive transactions—enabling them to exploit gaps in anti-money laundering (“AML”) and sanctions enforcement to launder money, finance corruption, and evade U.S. law.

The risks are real and urgent. Iran, North Korea, and Russia have turned to cryptocurrency and stablecoins to bypass international sanctions and move illicit funds, including through platforms with little or no Know Your Customer (“KYC”) compliance.¹ If the U.S. does not close the loopholes that can be exploited by these actors, the financial architecture advanced in GENIUS and CLARITY will further accelerate the growth of opaque and lawless financial networks.

The Problem: The Tether Loophole and Foreign Issuer Exemptions

Tether—the world’s largest stablecoin—has been repeatedly linked to illicit finance. Yet the GENIUS Act allows foreign issuers like Tether to remain active in U.S. markets via decentralized exchanges and peer-to-peer transfers, even if they fail to register as permitted issuers. While the bill bars such issuers from centralized exchanges after a three-year grace period, it provides Treasury with multiple mechanisms to issue waivers or exemptions. If a foreign issuer is located in a jurisdiction deemed “comparable,” or

¹ See, e.g., Angus Berwick and Tom Wilson, “Crypto exchange Binance helped Iranian firms trade \$8 billion despite sanctions,” Reuters, Nov. 7, 2022, <https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/>.

where the U.S. has a “reciprocity” agreement, their stablecoins may circulate freely—even on centralized exchanges. This loophole could serve as a backdoor for evading oversight.

The CLARITY Act no longer references stablecoins or digital assets at all. The removal of earlier provisions related to “covered payment stablecoins” and “covered digital assets” leaves the bill entirely silent on the role these financial instruments play in sensitive technology exports. Without explicit inclusion of digital assets or restrictions on their use in covered transactions, adversarial regimes may continue to finance access to U.S.-origin technologies using tools already tied to illicit finance and sanctions evasion.

The Solution: Amend both bills to:

- Define “issue” as “directly or indirectly, issue or otherwise make available for purchase, sale, or exchange”;
- Assign oversight of foreign issuers to a U.S. regulator such as the Comptroller of the Currency; and
- Ensure the CLARITY Act includes clear language affirming that digital assets and stablecoins used in connection with covered technology exports are subject to AML obligations under the Bank Secrecy Act (“BSA”).

The Problem: AML/CFT Gaps that Enable Corruption and Other Crime

While the GENIUS Act affirms that stablecoin issuers are subject to AML and countering the financing of terrorism (“CFT”) rules, this is already required under existing law. Critically, the bill does not extend AML/CFT obligations to the *secondary market*—such as digital asset exchanges, custodians, and brokers—where illicit actors obtain access to stablecoins. The result is a bill that affirms the status quo while ignoring how kleptocrats, terrorists, and other criminal actors access and move digital assets. Further, GENIUS weakens compliance by stating that issuers must follow AML rules only “as applicable”—a vague and unenforceable standard.

CLARITY repeats these same mistakes: It establishes regulatory expectations for financial instruments used in national security-sensitive transactions but does not impose AML/CFT program requirements on the key entities that move, exchange, or custody those assets. Without those controls, corrupt actors and sanctioned regimes will continue to exploit blind spots in the regulatory perimeter.

The Solution: Explicitly apply AML/CFT program obligations to digital asset exchanges, custodians, and brokers—not just issuers—that move or custody stablecoins, as well as related digital assets tied to sensitive technology sectors.

The Problem: Incomplete Sanctions Enforcement Tools

The GENIUS Act rightly grants the Secretary of the Treasury new authority to sanction foreign persons that engage in significant transactions involving covered payment stablecoins. However, it does not address other key vectors for sanctions evasion—such as anonymizing technologies (“mixers”) or non-issuer intermediaries who enable foreign actors to obscure the source and destination of funds. These omissions leave gaps in Treasury’s enforcement capacity.

The CLARITY Act fails to address sanctions evasion altogether. Despite the growing role of digital assets in sanctions circumvention, the bill contains no provisions referencing such instruments or authorizing enforcement tools to limit their misuse in sensitive exports. It includes no sanctions-screening requirements, no authority to act against non-compliant users, and no restrictions on anonymized or shielded transactions involving covered technologies.

The Solution: Retain GENIUS’s Section 7 sanctions authority and expand it to include anonymizing technologies and facilitating intermediaries, and amend CLARITY to authorize sanctions enforcement against the use of digital assets in covered transactions involving national security-sensitive technologies, including tools to identify, restrict, or penalize high-risk flows and anonymizing services.

The Problem: DeFi and Ownership Loopholes Will Undermine Enforcement

GENIUS permits so-called “decentralized” platforms to engage with noncompliant stablecoin issuers and exempts developers and operators from accountability. It also imposes no AML requirements on service providers.

CLARITY includes similar risks. It imposes no restrictions on beneficial ownership and provides no transparency or oversight regarding the use of opaque digital instruments in the financing of technology exports. It also creates no accountability for those who control or influence key components of the transaction infrastructure.

The Solution: Eliminate exemptions for decentralized services and platforms. Apply AML/CFT requirements to any party with control or influence over the financial infrastructure used to facilitate covered technology transactions. Require beneficial ownership disclosure across all entities involved in such transactions.

The GENIUS and CLARITY Acts must not entrench a regulatory framework that facilitates illicit finance and shields corruption. We urge Congress to adopt these essential amendments to protect U.S. national security and the integrity of the financial system.

Thank you for your consideration. If you have any questions, please contact Scott Greytak, Director of Advocacy for Transparency International U.S., at sgreytak@transparency.org.

Sincerely,

Transparency International U.S.
Free Russia Foundation
Financial Accountability and Corporate Transparency (“FACT”) Coalition
Nate Sibley, Kleptocracy Initiative, Hudson Institute

CC: Members of the U.S. House Committees on Financial Services, Homeland Security, and Foreign Affairs