

Law Enforcement, National Security, Anti-Scam, and Anticorruption Leaders Warn Congress That New Crypto Bill Leaves Dangerous Loopholes

The latest Senate cryptocurrency market structure bill would leave gaps that fraudsters, drug traffickers, sanctions evaders, transnational criminal organizations, terrorist financiers, corrupt foreign officials, and hostile foreign actors could exploit

A statement from Transparency International U.S.
May 13, 2026

WASHINGTON, D.C.—Tomorrow the Senate Banking Committee will consider a far-reaching cryptocurrency market structure bill that would establish a regulatory framework for digital asset markets, including rules governing digital asset intermediaries and the allocation of regulatory authority over certain digital assets and trading activity.

The scheduled Committee markup of the measure comes amid new and longstanding warnings from law enforcement, national security experts, anti-scam groups, anticorruption advocates, and other stakeholders that any such cryptocurrency legislation must not create carveouts that fraudsters, drug traffickers, sanctions evaders, transnational criminal organizations, terrorist financiers, corrupt foreign officials, and hostile foreign actors can exploit.

John Cassara, former U.S. Treasury Special Agent and anti-money laundering expert, said the following:

Crypto currencies are an increasingly important part of the money-laundering playbook for drug cartels, terrorist financiers, sanctions evaders, corrupt regimes, and scam networks. I spent my career following dirty money and value trails, and the lesson is simple: when Congress leaves gaps in the law, criminals and their enablers find and exploit them. Any crypto bill that fails to close major anti-money laundering loopholes both handicaps law enforcement and is a threat to our national security.

Richard Nephew, Former U.S. Coordinator on Global Anti-Corruption and Deputy Special Envoy for Iran, said the following:

At a time when we know that hostile actors like the IRGC are looking to circumvent US sanctions to rearm and threaten Americans and U.S. interests around the world, it is inconceivable to me that we would open new, effective channels for sanctions evasion.

Corey Frayer, Director of Investor Protection for the Consumer Federation of America, said the following:

Crypto has been exploding as the tool of choice for criminals targeting consumers with an onslaught of abuse from ransomware to romance scams. At a time when consumers need protection from fraud the most, it's baffling the Senate would consider weakening the laws and undercutting states' authority to fight back.

Alex Stapleton, Senior Policy Advisor for Foreign Policy for America, said the following:

Digital asset innovation cannot come at the expense of key national security and foreign policy tools the United States relies on to counter illicit finance. Any crypto legislation must include meaningful anti-money laundering and sanctions safeguards to prevent hostile regimes, terrorist financiers, and transnational criminal networks from exploiting gaps in the digital asset ecosystem. The current bill does not yet meet that standard.

Nate Sibley, former Director of the Hudson Institute's Kleptocracy Initiative, said the following:

Digital assets risk becoming the new frontier for laundering the proceeds of corruption, including bribery and embezzlement. Digital asset market structure legislation must incorporate robust provisions to protect against money laundering, sanctions evasion, and other illicit finance risks.

Debra LaPrevotte, former FBI Supervisory Special Agent, said the following:

During my career in law enforcement, I worked cases involving money laundering, corruption, and complex illicit finance networks. The lesson is clear: criminals exploit gaps wherever they find them. Congress should not pass cryptocurrency legislation that leaves major anti-money laundering loopholes unresolved or makes it harder for investigators to follow the money.

Karen Greenaway, retired FBI Supervisory Special Agent, said the following:

As a licensed attorney, retired federal law enforcement officer with a 22+ year career, and current law enforcement instructor and mentor to foreign law enforcement, prosecutors, and judges, there is no question that today the number one money laundering tool world-wide is cryptocurrency. Investigators and prosecutors from the more than 20 countries that I have trained are frustrated and often thwarted in their investigations and prosecutions because there are very few regulated cryptocurrency exchanges and even less that have a legal requirement to maintain financial records. In fact, one foreign investigator stated that cryptocurrency is often exchanged for cash in person-to-person transactions that are untraceable. The result is that terrorists, violent drug traffickers, and organized criminals who prey upon the elderly and unlearned in increasingly sophisticated financial and AI generated schemes are, quite literally, getting away with murder, funded by untraceable cryptocurrency transactions hidden behind an anonymous block chain.

Erin West, Founder of Operation Shamrock, a leading organization for educating about, mobilizing against, and disrupting the scam industry, said the following:

Crypto-enabled scams are already causing devastating losses for victims across the country, and criminals continue to exploit crypto ATMs and other high-risk channels to move stolen funds. Any crypto legislation that fails to preserve strong anti-money laundering obligations will make it harder for law enforcement to follow the money, recover funds, and stop these networks before they harm more people.

Gabe Lezra, Senior Policy Strategist at Democracy Defenders Action, said the following:

Crypto legislation is not just about market rules—it is about whether Congress will build guardrails against the next generation of dirty money. Without strong anti-money laundering safeguards, digital assets can become a gift to corrupt officials, sanctions evaders, fraudsters, and authoritarian networks looking to move money in the shadows. Congress should not pass a bill that makes it easier for criminals and kleptocrats to hide wealth, buy influence, or undermine democratic accountability.

Scott Greytak, Deputy Executive Director of Transparency International U.S. (TI US), said the following:

Congress should not pass crypto market structure legislation that leaves open new pathways for dirty money. The issue is not whether digital asset markets need rules; it is whether those rules will actually protect the U.S. financial system, help law enforcement follow the money, and prevent kleptocrats, fentanyl traffickers, ransomware crews, sanctions evaders, terrorist financiers, and hostile foreign actors from exploiting crypto platforms.

The needed safeguards are clear: Digital asset platforms should be covered by the Bank Secrecy Act. DeFi cannot become a law-free zone. Offshore platforms serving U.S. customers must follow U.S. AML and sanctions rules. And platforms that facilitate illicit activity should be cut off from the legitimate financial system.

The newly released draft does not meet that standard. Unless these gaps are closed, Congress risks allowing a market structure that gives criminals and corrupt actors more ways to move illicit funds while making it harder for investigators to trace money, recover stolen assets, and protect American communities.

Transparency International U.S. is part of the world's largest coalition against corruption. In collaboration with national chapters in more than 100 countries, we are leading the fight to turn our vision of a world free from corruption into reality.

Related Resources

- [Read](#) the text of the latest Senate Banking cryptocurrency proposal;
- [Read](#) a letter from a coalition of organizations committed to combating foreign corruption and kleptocracy urging lawmakers to address illicit finance gaps in cryptocurrency market structure legislation.

Media Contact

Victoria Brusa, Communications and Media Affairs, Transparency International U.S.
Telephone: +1 771 250-8065 / +54 9 3492 652098 (WhatsApp)
Email: vbrusa@us.transparency.org
Twitter: [@TransparencyUSA](https://twitter.com/TransparencyUSA)