TRANSPARENCY INTERNATIONAL U.S.
fighting corruption, promoting democracy

June 2026

Illicit Finance Gaps in the CLARITY Act

While some provisions of the CLARITY Act take steps to address illicit finance risks, the bill still leaves several important gaps that Congress must close. Market structure legislation should not create new pathways for digital asset businesses to serve U.S. customers, move dollar-denominated value, or profit from transaction activity while avoiding basic anti-money laundering (AML), sanctions, fraud-prevention, recordkeeping, and law enforcement response obligations. Those safeguards should be tailored to risk and capability, not imposed on ordinary users or neutral software development.

Section/Issue	Problem to Fix	Recommended Fix
Sec. 201. Clarify AML coverage for digital asset service providers.	The bill expands Bank Secrecy Act coverage for certain digital commodity brokers, dealers, and exchanges, but could still leave some digital asset service providers and other actors involved in facilitating digital asset transactions outside clear AML obligations. That could create uncertainty about which businesses must maintain AML programs, monitor for suspicious activity, and provide useful information to law enforcement.	Update the Bank Secrecy Act definition of "financial institution" to clearly cover the standard set of digital asset service providers reflected in FATF standards, including covered businesses that facilitate digital asset transactions, while preserving appropriate exclusions for users, validators, miners, and neutral software development. Congress can also direct Treasury to tailor requirements by risk, size, custody, customer relationship, and transaction role rather than impose bank-style obligations on every actor.
Sec. 202. Make examination standards additive, not duplicative.	Risk-based examination standards for virtual currency firms already exist and can be updated by regulators without new legislation. A new statutory mandate is useful only if it improves consistency across agencies and closes specific supervisory gaps rather than simply restating work already underway.	Direct regulators to update and harmonize existing examination procedures for digital asset activity, including expectations for suspicious activity reporting, sanctions screening, blockchain analytics, law-enforcement response, recordkeeping, and supervision of outsourced compliance functions.

Section/Issue	Problem to Fix	Recommended Fix
Sec. 203. Ensure information sharing builds on existing authorities.	The bill directs Treasury to create a new information-sharing pilot, but Treasury already administers public-private information-sharing programs under Section 314 of the USA PATRIOT Act. A new pilot should not recreate existing architecture or become a substitute for faster operational sharing with law enforcement.	Frame the pilot as an expansion of existing Section 314 information sharing for digital asset typologies. Require participation by relevant federal, state, and local law-enforcement agencies; provide feedback loops on SAR utility; and focus on time-sensitive fraud, sanctions evasion, ransomware, trafficking, and corruption-related laundering.
Sec. 204. Convert another study process into action on existing recommendations.	An interagency working group can be useful, but the government has already identified concrete digital asset illicit-finance gaps, including through Treasury's DeFi risk assessment and prior requests to Congress. The bill should not delay action by sending known problems back for more study.	Require Treasury, DOJ, and other agencies to report on implementation of existing recommendations and identify any remaining legislative text needed. Permit consultation with industry, civil society, law enforcement, victim advocates, and technical experts, while reserving final recommendations to government officials.
Sec. 205. Strengthen Crypto ATM protections and avoid treating kiosks as the whole scam problem.	Crypto ATMs are widely used in fraud schemes, including scams targeting older Americans, and the bill includes some useful safeguards. But most digital asset fraud losses occur through other channels, including online exchanges and other platforms. A kiosk-only approach leaves victims exposed and can push scammers toward less-protected channels.	Restore the strongest victim-protection provisions from the Crypto-ATM Fraud Prevention Act of 2025, including clear refund and disclosure rules. Extend appropriate anti-fraud, reporting, and victim-recovery safeguards to other digital asset service providers that scammers use to receive, move, or cash out proceeds.

Section/Issue	Problem to Fix	Recommended Fix
Sec. 301. Do not exempt commercially operated DeFi businesses from tailored AML duties.	The U.S. government has repeatedly warned that criminals exploit decentralized platforms to launder illicit funds. The bill's control-based framework risks excluding from AML obligations businesses that help build, promote, maintain, or profit from high-volume DeFi activity, even when those businesses have employees, substantial revenue, or practical ability to identify and mitigate illicit-finance risk.	Apply tailored AML duties to DeFi businesses above meaningful revenue, staffing, transaction-volume, or U.S.-activity thresholds. Duties should be scaled to actual risk and capability and may include suspicious activity reporting, sanctions compliance, law-enforcement response, risk assessments, and controls for known illicit wallets. Preserve clear protections for neutral software publishing, code auditing, infrastructure services, and ordinary users.
Sec. 302. Apply meaningful safeguards to interfaces that provide easy access to DeFi.	Websites, apps, and other interfaces are often the practical access point through which criminals and victims interact with DeFi. Non-binding guidance is not enough where an interface has an operator, earns revenue, serves U.S. users, or has practical ability to screen, warn, block, or report illicit activity. The bill also should not let foreign-run interfaces serve U.S. users while avoiding U.S. safeguards.	Require Treasury to impose tailored obligations on interface operators that meet meaningful revenue, traffic, U.S.-user, or transaction-facilitation thresholds. Covered interfaces should conduct risk assessments, screen against sanctions and high-risk wallet data where feasible, provide scam warnings, preserve relevant records, and report suspicious activity when they have useful information.
Sec. 303. Make the special measure effective against high-risk mixers and obfuscation tools.	A special measure that only limits certain regulated intermediaries may not deter direct use of the highest-risk mixers or other obfuscation services by criminals using self-hosted wallets or operating outside the United States. If the tool cannot create meaningful legal or sanctions risk around identified platforms, it may acknowledge the problem without isolating the highest-risk services.	Restore or clarify discretionary U.S. authority to impose effective sanctions or sanctions-like consequences on designated mixers, obfuscation services, and other platforms used to hide significant illicit activity. Ensure the measure reaches U.S. persons, U.S.-facing activity, and transactions that touch U.S. jurisdiction, while preserving due process and clear standards for designation and delisting.

Section/Issue	Problem to Fix	Recommended Fix
Sec. 304. Address stablecoin sanctions-enforcement risks rather than only studying them.	Dollar-backed stablecoins can allow foreign actors to pay sanctioned persons in dollar-denominated value without the transaction necessarily passing through ordinary dollar-clearing channels. A recurring report is useful, but it does not itself preserve the reach of U.S. sanctions power.	State clearly that transactions in U.S. dollar-backed stablecoins are subject to U.S. jurisdiction for sanctions-enforcement purposes when they involve U.S. issuers, U.S. persons, U.S. infrastructure, U.S.-facing services, or other constitutionally sufficient U.S. nexus. Require Treasury to issue implementing guidance and report on enforcement gaps.
Sec. 305. Pair temporary-hold safe harbors with affirmative victim-protection duties.	The bill gives digital asset firms and stablecoin issuers more comfort to voluntarily hold suspicious transactions or respond to law-enforcement requests. That is useful, but a safe harbor alone does not require firms to monitor for suspicious activity, honor lawful state and local requests, preserve funds, or return stolen assets to victims when a court orders restitution, seizure, or forfeiture.	Require issuers and covered digital asset service providers to maintain capability-based programs to detect and report suspicious activity, respond to lawful requests from federal, state, and local law enforcement, temporarily hold or preserve funds where legally required, and return stolen funds to victims pursuant to valid court orders. Require stablecoin issuers to monitor publicly visible blockchain activity involving their coins at a risk-appropriate level.
Sec. 307. Replace redundant authority language with concrete unhosted-wallet safeguards.	Treasury already has authority to issue guidance and regulations concerning monetary instruments and to assess risks from self-hosted or unhosted wallets. Language that merely restates discretion may add ambiguity without closing the operational gap: regulated firms need clear expectations for higher-risk transactions involving unhosted wallets.	Direct Treasury to require risk-based due diligence for covered firms' transactions involving unhosted wallets, including wallet-address collection where appropriate, sanctions and illicit-finance screening, enhanced due diligence for high-risk exposure, recordkeeping, and suspicious activity reporting. Avoid language that unintentionally narrows Treasury's existing authority.

Section/Issue	Problem to Fix	Recommended Fix
Sec. 308. Do not acknowledge DeFi risk only at the point of routing.	Requiring regulated intermediaries to apply risk-management standards before routing transactions through DeFi recognizes that DeFi can present elevated illicit-finance risk. But the same risk should not be addressed only when a regulated intermediary touches the transaction; otherwise, the bill encourages activity to migrate to channels where no covered intermediary is present.	Keep the intermediary risk-management requirement, but pair it with tailored obligations for covered DeFi businesses and interfaces. Require Treasury to define practical standards for routing, counterparty due diligence, high-risk protocol exposure, and suspicious activity reporting.
Sec. 507. Promote global standards by meeting them at home.	The bill directs Treasury to work with foreign counterparts on counter-illicit-finance standards, which is already a core Treasury function. That diplomatic effort will be stronger if U.S. law clearly meets or exceeds the FATF baseline for virtual assets, including appropriate coverage of digital asset service providers and certain DeFi arrangements.	Align U.S. law with FATF virtual-asset standards and avoid domestic exemptions that could weaken U.S. credibility abroad. Direct Treasury to use bilateral and FATF engagement to press other jurisdictions to supervise offshore platforms, require registration or licensing where appropriate, and close gaps exploited by ransomware, sanctions evasion, trafficking, fraud, and corruption networks.
Sec. 604. Protect genuine developers without creating overly broad exemptions from illicit finance safeguards.	The bill's developer protections are important, but the current exemption could be interpreted broadly enough to cover businesses that do more than publish code or provide neutral infrastructure. Drawing the line only around custody or control of user assets can miss businesses that facilitate, route, promote, or profit from value transfer while maintaining practical ability to mitigate illicit finance risk.	Create a clear safe harbor for neutral software development and infrastructure, including oracles, node providers, data feeds, identity tools, cybersecurity services, and code auditors. Separately cover businesses that operate, administer, materially facilitate, or derive significant commercial benefit from transaction activity above meaningful thresholds, with obligations tailored to their role and capability.

Section/Issue	Problem to Fix	Recommended Fix
Cross-cutting gap. Prevent offshore platforms from avoiding U.S. law while serving U.S. markets.	The bill should not allow a platform to avoid U.S. illicit-finance law simply by locating headquarters, servers, or formal corporate entities offshore while serving U.S. customers, marketing to U.S. users, using U.S. infrastructure, or causing substantial effects in the United States.	Apply U.S. AML and sanctions obligations to foreign digital asset platforms that conduct significant U.S. business, serve U.S. customers, use U.S. infrastructure, or otherwise have a sufficient U.S. nexus. Provide clear standards so legitimate firms know when U.S. rules apply.
Cross-cutting gap. Ensure fraud victims can recover assets when funds are traceable.	Digital asset fraud often moves quickly, but blockchain tracing can identify funds before they are fully cashed out. The bill should not rely only on voluntary cooperation by firms, especially where victims have court orders or law enforcement has identified traceable stolen assets.	Require covered firms and stablecoin issuers to maintain procedures for timely preservation and return of traceable stolen assets when required by lawful process, including court orders for seizure, forfeiture, restitution, or victim return. Clarify that good-faith compliance with lawful process does not create undue liability.
Cross-cutting gap. Preserve records and rapid law-enforcement response.	Many digital asset investigations depend on fast access to records, wallet information, account identifiers, IP logs, device information, and transaction histories. Without clear retention and response requirements, law enforcement can lose the trail before victims recover funds or prosecutors identify bad actors.	Require covered digital asset firms to maintain risk-based records and a 24/7 or otherwise timely law-enforcement response process for urgent fraud, sanctions, terrorism, ransomware, trafficking, and corruption-related cases. Tailor requirements by firm size, activity, custody, and risk.

For more information, please contact TI US's Deputy Executive Director, Scott Greytak, at sgreytak@us.transparency.org.