

Securities Regulation Daily Wrap Up, BLOCKCHAIN—Bank Policy Institute: Anti-money laundering loopholes undermine effective regulation of digital assets, (Nov. 5, 2025)

Securities Regulation Daily Wrap Up

[Click to open document in a browser](#)

By A. Bryan Gerepka

Illicit actors and sanctioned parties are relying on un-hosted and non-U.S.-hosted wallets, as well as utilizing DeFi applications, to evade detection and exploit the U.S. financial system, the group stated.

Policymakers should ensure that digital asset intermediaries engaged in substantially similar activities as banks are subject to equivalent anti-money laundering (AML) standards, especially the “Know Your Customer” (KYC) rule, according to a report issued by the Bank Policy Institute (BPI), a bank trade group. If these gaps are not addressed through regulations or via market structure legislation, BPI [warned](#), proceeds of money laundering and terrorist financing may contaminate the U.S. digital asset ecosystem, including through payment stablecoin transactions, and eventually the more regulated “traditional” financial system.

Gaps in KYC reviews. The report highlighted the KYC as a particular area of concern. Under KYC, banks and other regulated financial institutions are legally required to verify the identity of every new customer before opening an account by collecting the customer’s name, address, date of birth, and a photo ID. Additionally, banks and regulated financial institutions are required to monitor the movement of money into and out of those accounts to ensure they do not facilitate illicit finance.

While the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act requires stablecoin issuers, as well as digital asset intermediaries—such as exchanges and hosted wallet providers—to comply with KYC and certain AML requirements, BPI [observed](#) that the requirements are less than those imposed on banks.

KYC requirements are essential first steps in combating illicit finance in the digital asset world, the group stated. While digital asset transactions may be publicly transparent on the blockchain, the identities of the individuals or companies behind them may remain entirely unknown, the group noted.

Risks posed by un-hosted digital platforms. BPI highlighted discrepancies in AML standards on hosted versus un-hosted platforms as a potential source of contagion in the traditional banking system. A hosted wallet is a service offered by a bank or other regulated entity that is subject to KYC rules. An un-hosted wallet is software, downloadable online and not associated with a KYC-compliant institution, the report stated. While the GENIUS Act requires AML compliance, BPI warned that stablecoin transactions between hosted wallets offered by KYC-compliant financial institutions must be properly vetted for illicit transactions.

Pathways to illicit financing. BPI identified three types of transactions that would allow potential bad actors to use payment stablecoins or other cryptocurrencies to conduct illicit activities:

- (1) Offshore-hosted wallets at a non-U.S. exchange, which may not be subject to the same KYC requirements as their U.S. counterparts.
- (2) Transactions between hosted and un-hosted wallets that are not subject to KYC requirements. For example, regulated financial institutions must comply with the “travel rule” under the Bank Secrecy Act, which requires institutions to maintain records for five years on money transfers that exceed \$3,000. This requirement was implemented in 1996 as part of the BSA, the report stated. Such a requirement is needed in the digital assets space, as the involvement of an un-hosted wallet could deprive a regulated financial institution of information about digital assets and their sources that is important in detecting illicit activity.

- (3) DeFi protocols, where hosted wallets may also potentially interact with certain DeFi protocols, which by design are decentralized and lack a central authority to administer KYC and other compliance requirements. These protocols may be used to evade illicit finance controls, the report noted. Some examples of DeFi protocols include “crypto mixers”, which combine clean and illicit digital assets to obscure the chain between a cryptocurrency’s source and its destination. Similarly, decentralized exchanges allow crypto users to trade and transact stablecoins or crypto directly without corresponding illicit finance safeguards. These DeFi protocols may allow terrorist financiers, money launderers, and drug traffickers to facilitate criminal activity.

Illicit actors and sanctioned parties are relying on un-hosted and non-U.S.-hosted wallets, as well as utilizing DeFi applications, to evade detection and exploit the U.S. financial system, BPI warned. These persistent gaps in the regulated digital assets illicit finance framework undermine the safeguards of AML requirements, including those established by the GENIUS Act, and hinder law enforcement and national security experts’ ability to combat crime. Congress and regulators should address this critical gap in AML requirements, the report concluded.

Companies: Bank Policy Institute

IndustryNews: Blockchain FinancialIntermediaries