TRANSPARENCY INTERNATIONAL U.S.
fighting corruption, promoting democracy

CRYPTO'S DIRTY MONEY PROBLEM: WHAT CONGRESS MUST FIX

By Scott Greytak & Annalise Burkhart
July 2026

EXECUTIVE SUMMARY

Cryptocurrency is no longer a fringe financial technology. It is a fast-moving, global payment and settlement system used by consumers, companies, investors, and developers. And it's also a system increasingly used by criminals, kleptocrats, sanctions evaders, terrorist financiers, ransomware groups, scammers, and corrupt officials who need to move value quickly, across borders, and outside the ordinary legal architecture of the traditional financial system.

The policy question in 2026 is not whether digital assets should exist. They do. Rather, the question is whether governments will bring their use within a regulatory framework that reflects the most obvious lesson of modern financial crime: Illicit actors follow the path of least resistance. If the Bank Secrecy Act, the core U.S. law for stopping dirty money, applies when a person moves money through the traditional financial system but does not clearly apply when the same function is performed through digital asset software, offshore platforms, self-custodied wallets, decentralized protocols, mixers, or stablecoin rails, the law has not kept pace with the risk. It has opened—and given the presumption of legal cover to—a laundering channel.

The risks are now well documented. The U.S. Department of the Treasury has identified digital asset-related risks in its national illicit finance work, from the misuse of digital asset kiosks and hacks of digital asset service providers to foreign terrorist fundraising and other criminal activity.[i] Treasury's risk assessment of decentralized finance, or DeFi, found that illicit actors are abusing DeFi services and that many services invoke decentralization while failing to comply with anti-money laundering and countering-the-financing-of-terrorism (AML/CFT) obligations.[ii] The Financial Action Task Force, or *FATF*, the leading global anti-money laundering standard-setter, has likewise warned that gaps in one jurisdiction can have global consequences because virtual assets move across borders by design. FATF's 2026 report on stablecoins—digital assets designed to maintain a stable value, often by being pegged to a currency like the U.S. dollar—underscores that risk and highlights their misuse through unhosted wallets, peer-to-peer transactions, and other channels.[iii]

The scale is significant, even if no single estimate captures it precisely. Chainalysis, for example, reported that illicit cryptocurrency activity reached record highs in 2025 and that nation-state sanctions evasion increasingly relied on digital assets.[iv] TRM Labs estimated $158 billion in illicit crypto flows in 2025, while also noting that illicit activity declined as a share of total crypto volume from 2024 to 2025.[v] These are private sector estimates, not government statistics, and should be understood as directional rather than definitive. But they reinforce what Treasury and law enforcement actions already show: Digital assets are now part of the infrastructure of modern financial crime.

As the U.S. Congress considers legislation to define the future of digital asset markets, this report seeks to show what is at stake if illicit finance is treated as an afterthought. Regulatory clarity is necessary, but regulation that leaves gaps for money laundering, sanctions evasion, terrorist financing, trafficking, fraud, and corruption is not a serious framework.

This report identifies three core concerns:

1. Cryptocurrency presents real illicit finance risks because it combines speed, scale, pseudonymity, global reach, uneven

regulation, and new mechanisms for hiding or moving funds. Those features are not inherently criminal. But they are attractive to criminals when not matched by serious compliance obligations.

2. Stablecoins have become especially important. Their value stability, liquidity, dollar denomination, use across exchanges, DeFi protocols, and peer-to-peer channels make them useful for legitimate commerce. But these same features also make them attractive for sanctions evasion, scam payments, terrorist financing, trafficking networks, and the laundering of the proceeds of corruption.
3. Congress should not pass crypto market structure legislation that delivers regulatory clarity for industry while leaving law enforcement, Treasury, financial institutions, and covered digital asset firms without the tools they need to detect, trace, and disrupt illicit finance. A framework that clarifies the rules for markets, but weakens the rules against dirty money, is not real reform. It is an invitation to abuse.

Any serious crypto bill must meet a basic test: Does it follow the risk? That means applying AML/CFT obligations based on financial function, not labels; covering digital asset service providers consistent with global standards while protecting ordinary users, validators, miners, and neutral software development; closing offshore escape hatches; addressing DeFi businesses and interfaces where identifiable people or entities exercise control, material influence, or significant commercial benefit; covering stablecoin issuers and the risks they are positioned to see; clarifying authority over mixers and other anonymizing services; imposing risk-based safeguards for exposure to unhosted wallets; preserving sanctions authority for dollar-backed stablecoins and other digital asset activity with a sufficient U.S. nexus; strengthening fraud prevention, victim recovery, recordkeeping, information sharing, and rapid law-enforcement response; and giving Treasury, the U.S. Department of Justice (DOJ), the Criminal Investigation division of the Internal Revenue Service, the Federal Bureau of Investigation, and state and local law enforcement the resources needed to enforce the rules.

I. THE ILLICIT FINANCE RISK IS NOT THEORETICAL

For years, crypto illicit finance debates were often trapped between two slogans. Industry defenders said blockchain transparency made crypto a bad tool for crime. Critics said crypto was only for crime. Both positions were too simple.

Public blockchains can create useful investigative trails. Like traditional financial institutions, law enforcement has repeatedly traced funds, seized assets, and built cases using account information whether by following bank records or blockchain analytics. Both hold real advantage compared with cash and informal value transfer systems. But, transparency of transactions is not the same thing as a compliance program, and tracing after the fact is not a substitute for obligations that help prevent, detect, report, and stop illicit activity in real time. A transaction can be visible on a blockchain and still involve an unidentified actor, an anonymous company, an offshore exchange, a mixer, a self-custodied wallet, a sanctions target, a hacked account, or a protocol with no meaningful AML program.

The problem is not that every digital asset transaction is suspicious. It's that, without proper protocols, digital asset systems allow value to move in ways that can outrun the legal obligations that normally attach to financial intermediaries. That gap matters

most when the transaction is not a speculative trade, but the movement of ransomware proceeds, bribe money, stolen public assets, fraud proceeds, sanctions-evasion funds, narcotics proceeds, or money controlled by foreign terrorist organizations.

For example, the Binance case showed what happens when a major global crypto platform fails to build a lawful compliance program around massive transaction volume. In 2023, Binance and its founder pleaded guilty in a resolution involving more than $4 billion in penalties.[vi] DOJ stated that Binance failed to prevent and report suspicious transactions and failed to register as a money transmitting business; Treasury described related Bank Secrecy Act (BSA) and sanctions violations involving terrorists, ransomware attackers, money launderers, and other criminals.[vii] That case was not a theoretical debate about code. It was a basic AML failure at truly global scale.

Other cases and advisories point in the same direction. The Financial Crimes Enforcement Network, or FinCEN, the Treasury bureau responsible for safeguarding the U.S. financial system from money laundering, terrorist financing, and other illicit finance threats, warned about convertible virtual currency kiosks being used for scam payments and other illicit finance.[viii] And FinCEN's fentanyl-related financial trend analysis identified approximately $1.4 billion in suspicious crypto transactions in 2024 BSA reporting tied to suspected fentanyl-related activity, while also highlighting the role of financial intelligence in mapping threat patterns.[ix]

HOW CRYPTO HAS ENABLED TERRORIST FINANCING

The DOJ's 2020 disruption of three terrorism-finance cyber-enabled campaigns is an example of cross-platform, multi-group enforcement involving cryptocurrency wallets, websites, and donation channels.[x] The policy lesson from this case is important: Blockchain analytics and public-private tracing are useful, but they work best when paired with clear reporting duties, reliable records, sanctions controls, and rapid law-enforcement response.

a. **Hamas/al-Qassam Brigades.** Hamas-related crypto fundraising campaigns have been identified, and Hamas's military wing publicly moved away from Bitcoin fundraising after tracing and enforcement pressure.
b. **Al-Qaeda.** Al-Qaeda and affiliated terrorist groups largely operating out of Syria used sham charities and solicited cryptocurrency donations via Telegram channels for weapons procurement before being disrupted by law enforcement.
c. **ISIS/ISKP.** The Islamic State (ISIS) and its affiliate, the Islamic State Khorasan Province (ISKP), have used cryptocurrency for fundraising, including through privacy-enhancing assets and online donation campaigns. These examples support covering peer-to-peer and unhosted wallet exposure where businesses interact with suspicious activity.

In May 2026, FinCEN warned that the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and its proxies use front companies, financial facilitators, and digital assets to support sanctions evasion and money laundering.[xi] In June 2026, Treasury sanctioned Nobitex, Iran's largest digital asset exchange, and other Iranian digital asset exchanges for alleged terror finance and sanctions evasion activity.[xii] The evidence of Iranian and IRGC-linked digital asset activity, including the use of exchanges and front-company networks, supports requiring stablecoin issuers, exchanges, and digital asset intermediaries to maintain operational sanctions controls, not merely formal written policies.

These examples are not identical. They involve different technologies, actors, jurisdictions, and legal theories. But they share one feature: Digital assets are being used in the real world to move value for serious crime and national security threats. A responsible legislative framework must start there.

Digital assets are particularly attractive to illicit actors for at least six important reasons:

1. **Speed.** Crypto transactions can move value quickly, including across borders and outside banking hours. That speed is useful for legitimate payments, but also for fraud rings, ransomware actors, sanctions evaders, and corrupt networks trying to move funds before authorities can intervene.
2. **Pseudonymity.** Many blockchain addresses are public, but the person behind the address may not be known. A corrupt official does not need perfect anonymity. Often, the official needs only enough separation between name, wallet, nominee, company, exchange account, and asset to create friction for investigators.
3. **Borderless access.** Digital assets can be moved through platforms and protocols based in multiple jurisdictions. FATF has repeatedly warned that uneven implementation of virtual asset standards creates cross-border vulnerabilities.[xiii]
4. **Regulatory arbitrage.** Illicit actors can route funds through offshore platforms, decentralized protocols, weakly supervised services, peer-to-peer channels, or intermediaries that claim they are not covered by existing AML rules.
5. **Obfuscation tools.** Mixers, chain-hopping, bridges, nested services, peel chains, high-velocity wallets, and other techniques can complicate tracing and attribution.
6. **Dollar-like stability.** Stablecoins allow actors to move value in digital form without taking on the volatility of Bitcoin or other assets. FATF has warned that stablecoins' characteristics can make them attractive for misuse in money laundering, terrorist financing, sanctions evasion, and proliferation financing.[xiv]

None of these features means that digital assets should be prohibited. Rather, it means that digital asset legislation should be built with the same realism that underlies every other serious financial crime law. If a product can move money, store value, hide ownership, or facilitate access to the financial system, illicit actors will test it.

HUMAN TRAFFICKING, FORCED-CRIMINALITY SCAM COMPOUNDS, AND CHILD SEXUAL ABUSE MATERIAL

A serious bill should treat human trafficking, forced labor, child sexual abuse material (CSAM), fraud, and crypto laundering as connected problems. AML/CFT obligations should require red-flag detection for scam typologies, high-risk corridors, and suspicious clustering of wallets, accounts, and over-the-counter (OTC) activity. These examples reinforce that crypto AML/CFT rules are not only about banks or national security; they affect the ability to identify and disrupt the worst forms of online exploitation, including transnational abuse networks.

a. **Southeast Asian scam compounds.** Pig-butchering operations—investment scams where the perpetrator gains the trust of the victim over time—have been linked to human trafficking and forced criminality in scam compounds, including networks where victims are forced to run online investment scams and process crypto payments.
b. **Welcome to Video.** Welcome to Video is a central CSAM case involving cryptocurrency payments and blockchain tracing.[xv] Law enforcement used Bitcoin transaction analysis to identify users and administrators across jurisdictions.
c. **Kidflix, Cryptomus, Alice with Violence CP, Bitcoin Fog, and Chainalysis investigations.** These examples show how cryptocurrency can be used in CSAM-related payment systems, processors, fraudulent CSAM-advertising schemes, and laundering tools. They also show the other side of the ledger: blockchain tracing and financial intelligence can help law enforcement identify users, administrators, payment infrastructure, and laundering channel.[xvi]

II. STABLECOINS ARE BECOMING A CENTRAL ILLICIT FINANCE CONCERN

Stablecoins deserve special attention because they are becoming one of the most important bridges between crypto markets and the broader dollar-based financial system. They can function as settlement instruments for trading, collateral, payments, remittances, DeFi transactions, and offshore value movement.

Their appeal is obvious: They are designed to hold a stable value, often by referencing the

U.S. dollar; they can move at blockchain speed; and they can be used across platforms and jurisdictions.

That is also why illicit actors like them. A dollar-referenced token that can be transferred globally, held outside the banking system, and used on exchanges or in DeFi can be extremely useful for moving and obfuscating funds. FATF's 2026 targeted report on stablecoins and unhosted wallets highlights the misuse of stablecoins through peer-to-peer transactions and discusses indicators of stablecoin misuse.[xvii] And Chainalysis has reported that stablecoins account for a growing share of illicit transaction volume.[xviii]

The GENIUS Act, the federal framework governing payment stablecoin issuers, was a milestone because it requires permitted payment stablecoin issuers to be treated as financial institutions for BSA purposes and subject to federal laws relating to sanctions, prevention of money laundering, customer identification, and due diligence.[xix] That is a necessary baseline. But issuer-level regulation cannot be the end of the conversation.

Stablecoin risk does not stop at issuance. Once a stablecoin enters secondary markets, it can move through hosted wallets, unhosted wallets, centralized exchanges, decentralized exchanges, bridges, mixers, lending protocols, OTC brokers, sanctions-evasion networks, and high-risk foreign platforms. A stablecoin issuer may not control every downstream transfer, but issuers often have visibility, contractual powers, technical capabilities, redemption controls, blacklist or freeze functions, and market intelligence that can help detect and disrupt illicit finance. Legislation and implementing rules should require reasonable, risk-based ecosystem monitoring and responsive controls, not just onboarding checks for direct customers.

Congress should preserve and build on the GENIUS Act's illicit finance framework in any new cryptocurrency legislation. Stablecoin issuers should remain subject to risk-based AML/CFT and sanctions obligations, including customer identification, suspicious activity reporting, sanctions screening, transaction monitoring, redemption controls, law enforcement cooperation, and technical capacity to block, freeze, or reject unlawful transactions.

III. DEFI AND SOFTWARE-BASED FINANCE CANNOT BE CATEGORICALLY EXEMPTED FROM ILLICIT FINANCE OBLIGATIONS

Not all decentralized finance protocols are alike. Some protocols are genuinely decentralized and difficult for any person to control after deployment. Others have identifiable developers, administrators, front-end operators, relayers, sequencers, fee recipients, foundations, companies, or governance arrangements through which identifiable people or entities exercise control or material influence over how users access the service and how risk can be mitigated. A serious legal framework must distinguish between passive publication of code and the operation of financial services.

Treasury's 2023 DeFi risk assessment found that illicit actors, including ransomware actors, thieves, scammers, and North Korean cyber actors, use DeFi services in the process of laundering illicit funds, and that some DeFi services fail to comply with existing AML/CFT obligations.[xx] The assessment also made clear that claims of decentralization do not automatically determine legal status. That principle should guide Congress.

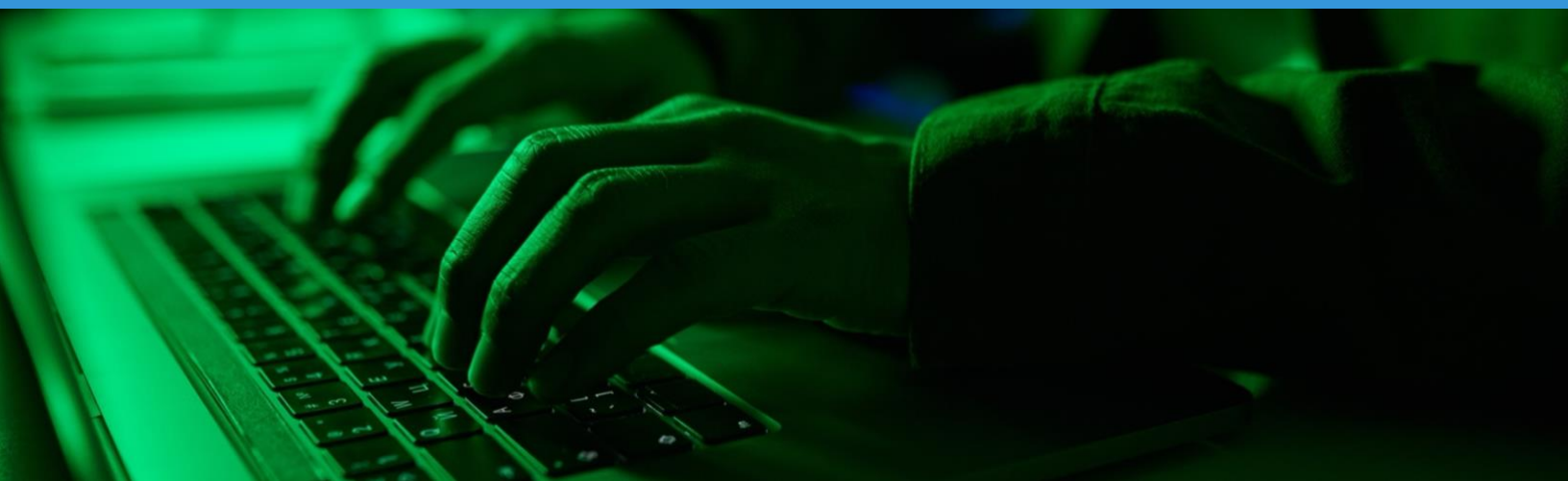
The law should apply based on function and control: If a person or business facilitates digital asset exchange, transfer, custody, settlement, lending, mixing, or other financial activity, and has the practical ability to control, administer, profit from, materially influence, or mitigate the illicit-finance risk of the service, then tailored AML/CFT obligations should attach. Those obligations should not apply merely because someone publishes neutral software, validates transactions, audits code, provides infrastructure, or uses a service as an ordinary user.

At the same time, Congress should avoid overbroad language that sweeps in neutral software publication, ordinary users, or persons with no ability to control a service or mitigate risk. The goal is not to criminalize code. It is to prevent financial activity from being deliberately structured so that nobody is responsible for compliance.

RANSOMWARE AND EXTORTION

BSA filings and FinCEN trend analyses are valuable for identifying ransomware patterns, payment methods, and laundering routes. Suspicious Activity Report (SAR) obligations should be preserved and information-sharing strengthened rather than weakening reporting under a "burden reduction" frame.

a. **Colonial Pipeline/DarkSide.** Colonial Pipeline remains the core example of ransomware against critical infrastructure. Colonial paid 75 BTC, and DOJ later announced the recovery of 63.7 BTC.[xxi] The example cuts both ways: crypto enabled rapid ransom payment, but the public blockchain and law-enforcement access to the wallet allowed partial recovery. The lesson is not that crypto is untraceable; it is that tracing must be matched with resources, reporting, and off-ramp controls.
b. **WannaCry/Lazarus Group.** WannaCry was a North Korea-attributed ransomware worm that infected hundreds of thousands of computers globally and demanded payment in Bitcoin.[xxii] The case shows that state actors can deploy ransomware and cryptocurrency extortion at global scale, even when the direct ransom haul is modest compared with total damage.
c. **REvil/Kaseya.** The Kaseya attack shows how ransomware can scale through software supply chains and managed service providers. REvil's use of Bitcoin and Monero, large ransom demands, international enforcement, seizures, and prosecution of affiliates make the case a useful example of both the threat and the enforcement response.[xxiii]
d. **Hive, LockBit, ALPHV/BlackCat, Cl0p, DarkSide, REvil, and other ransomware groups.** These groups show that ransomware is not a one-off problem but a recurring business model. Crypto is the payment layer that lets affiliates, operators, and laundering services divide and move proceeds across borders.



IV. MIXERS, OBFUSCATION SERVICES, AND SANCTIONS TOOLS NEED CLEAR STATUTORY FOOTING

Mixers and anonymizing services present one of the hardest policy questions in crypto. Services that are designed to sever the link between source and destination of funds can be abused by serious criminal actors.

Treasury sanctioned Tornado Cash in 2022, stating that it had been used to launder more than $7 billion worth of virtual currency since 2019, including more than $455 million stolen by the Lazarus Group, a state-sponsored hacking group alleged to be affiliated with the North Korean government.[xxiv] In 2024, the U.S. Court of Appeals for the Fifth Circuit held in Van Loon v. Department of the Treasury that certain immutable Tornado Cash smart contracts were not "property" under IEEPA and therefore could not be sanctioned on the theory used by OFAC.[xxv] Tornado Cash is legally and policy-significant because it used immutable smart contracts and raised hard questions about sanctions authority, developer liability, and how to address privacy-preserving code when it is also used for large-scale laundering. OFAC later delisted Tornado Cash following the decision.[xxvi]

High-risk services used to hide the proceeds of serious crime cannot sit outside effective sanctions, AML, and law-enforcement tools simply because they are software-based. Sanctions, AML, and law enforcement tools should not turn on whether a laundering mechanism happens to be implemented through immutable smart contracts rather than a company's bank account. Nor should Treasury be forced to stretch old statutory language beyond recognition. Congress should provide clear authority, with appropriate safeguards, to address digital asset mixers, anonymizing services, and other obfuscation mechanisms when they are used to facilitate money laundering, sanctions evasion, terrorist financing, proliferation financing, ransomware, or other serious illicit finance.

That authority should be carefully drafted. It should target covered conduct and services, not mere privacy research or publication of open-source code. It should preserve lawful privacy tools where risk can be managed. But it should not leave Treasury and law enforcement powerless against laundering infrastructure simply because the infrastructure is software-based.

FRAUD, SCAMS, RUG PULLS, PONZI SCHEMES, AND PIG-BUTCHERING

Investment fraud. Crypto investment fraud is one of the largest categories of consumer harm. The lesson is that illicit finance policy should not treat fraud as separate from AML; fraud proceeds must be laundered and cashed out.

Crypto-to-cash desks. Cash desks, including in Hong Kong and other hubs, are physical-world off-ramps that can convert crypto into cash with limited transparency. These desks connect online fraud, pig-butchering, trafficking compounds, and money laundering.

Pig-butchering. Pig-butchering is linked to crypto payment rails, social engineering, fake trading platforms, scam compounds, and human trafficking. This is one of the strongest bridges between consumer protection, trafficking, corruption, and AML.

Rug pulls. Rug pulls are schemes in which promoters attract liquidity or investment and then abandon the project or drain value, and are a recurring DeFi and token-launch risk.

V. CORRUPTION-SPECIFIC RISKS: CRYPTO AS THE NEW OFFSHORE ACCOUNT

Corruption is a money movement problem. Bribes, kickbacks, embezzled public funds, illicit campaign support, procurement fraud, sanctions-evasion revenue, and stolen state assets all need to be placed, layered, and integrated. Historically, corrupt actors relied on shell companies, private banks, luxury real estate, art, lawyers, accountants, and offshore secrecy jurisdictions. Those tools still matter. Crypto adds another layer.

Crypto can help corrupt actors in at least five ways:

1. It can move value quickly across borders before authorities can freeze funds.
2. It can allow corrupt officials, family members, or close associates to use wallets, nominees, offshore exchanges, or front companies to obscure beneficial ownership.
3. It can enable sanctions evasion by regimes, state-linked actors, or politically connected networks seeking access to dollar-like value outside traditional banks.
4. It can help corrupt networks convert cybercrime, fraud, trafficking, or procurement proceeds into assets that can later be cashed out through exchanges, OTC brokers, luxury purchases, or real estate.
5. It can create new conflicts of interest when public officials or their families own, promote, sponsor, or profit from digital asset ventures while the government writes or enforces the rules governing the industry.

FinCEN's national AML/CFT priorities include corruption, cybercrime, fraud, terrorist financing, transnational criminal organization activity, drug trafficking, human trafficking, proliferation financing, and sanctions evasion.[xxvii] Crypto is relevant to all of these listed priorities. A digital asset bill that treats AML as an afterthought would fail the basic national security and anticorruption test.

This is especially important for foreign kleptocracy and sanctions evasion. FinCEN's May 2026 IRGC alert describes the use of front companies, financial facilitators, and digital assets by the IRGC-Qods Force and its proxies.[xxviii] Treasury's June 2026 sanctions against Iranian digital asset exchanges likewise demonstrate how digital asset platforms can become part of state-linked sanctions evasion infrastructure.[xxix] These are corruption risks as well as national security risks: authoritarian regimes use financial opacity to protect regime wealth, fund coercive activity, and shield politically connected networks.

Crypto also enables tax evasion and offshore concealment. Crypto can be used to move or store value outside traditional account-reporting channels, and unreported crypto gains are a recurring tax compliance problem, particularly where taxpayers use offshore exchanges, self-custodied wallets, DeFi protocols, or mixers to obscure activity.

VI. WHAT A SERIOUS CRYPTO BILL MUST DO

Congress should not pass digital asset market structure legislation that treats illicit finance as a secondary implementation detail. The bill itself should contain clear statutory requirements. Below are the minimum elements.

1. Apply AML/CFT obligations based on financial function, not labels

The bill should establish a functional test for covered digital asset activity. A person should not escape AML/CFT obligations by describing

the activity as decentralized, offshore, non-custodial, software-only, a protocol, or a front end if the person is functionally providing or facilitating financial activity and has the practical ability to manage illicit finance risk.

Illustrative language: "A person that, for compensation or other commercial benefit, provides, administers, controls, materially facilitates, or materially influences a digital asset service that enables the exchange, transfer, custody, settlement, lending, mixing, issuance, redemption, or other movement of value shall be subject to applicable AML/CFT and sanctions obligations to the extent the person has the practical ability to identify, assess, mitigate, prevent, or report illicit finance risk."

The bill should make clear that the test turns on function, benefit, control, and capacity to mitigate risk. It should also protect truly passive actors.

Illustrative language: "Nothing in this section shall be construed to impose AML/CFT obligations solely on a person for publishing software code, validating transactions without customer-facing activity, or using a digital asset service as an end user, absent control, administration, compensation tied to the covered service, or practical ability to mitigate illicit finance risk."

2. Close offshore escape hatches

Digital asset platforms should not be able to serve U.S. customers, market to U.S. users, use U.S. infrastructure, or access U.S. markets while avoiding U.S. AML and sanctions obligations by incorporating abroad. The Binance resolution showed the danger of large global platforms failing to comply with U.S. AML and sanctions law while serving U.S. users and processing high-risk transactions.[xxx]

Illustrative language: "A digital asset service shall be subject to this Act and to applicable AML/CFT and sanctions obligations if it knowingly or recklessly serves U.S. persons, markets services to U.S. persons, conducts substantial activity through U.S. infrastructure, uses U.S. correspondent or settlement relationships, or facilitates transactions involving payment stablecoins issued by U.S.-regulated issuers, unless exempted by regulation."

3. Require stablecoin issuers to monitor ecosystem risk

Stablecoin legislation should not stop at direct customer onboarding. Permitted payment stablecoin issuers should be required to implement risk-based programs that account for the ways their tokens move in secondary markets, including through exchanges, DeFi protocols, bridges, mixers, and high-risk jurisdictions. FinCEN's and OFAC's proposed GENIUS Act rule already recognizes that permitted payment stablecoin issuers must be treated as financial institutions for BSA purposes and be subject to sanctions-related requirements.[xxxi] Congress should preserve and strengthen that approach.

Illustrative language: "A permitted payment stablecoin issuer shall maintain a risk-based AML/CFT and sanctions compliance program that includes reasonable monitoring of illicit finance risks involving the issuer's payment stablecoins in primary and secondary markets, including risks involving sanctioned persons, terrorist financing, proliferation financing, ransomware, fraud, trafficking, corruption-related proceeds, mixers, high-risk foreign platforms, and other typologies identified by the Secretary."

Illustrative language: "Such program shall include, as appropriate, customer identification and due diligence for direct customers; suspicious activity reporting;

sanctions screening; transaction monitoring; redemption controls; law enforcement response procedures; and technical or contractual controls, including freezing, blocking, burning, deny-listing, or other risk mitigation measures where lawful and practicable."

4. Cover DeFi businesses and interfaces where identifiable persons control, influence, or materially benefit from the service

The bill should not pretend that every DeFi arrangement is the same. Some systems may have no administrator after deployment. Others are operated through companies, foundations, interfaces, governance arrangements, relayers, sequencers, or other identifiable control points. Treasury's DeFi risk assessment provides the basis for this distinction and warns against illicit actors exploiting gaps in AML/CFT coverage.[xxxii]

Illustrative language: "A person shall not be exempt from AML/CFT or sanctions obligations solely because a digital asset service uses smart contracts, distributed ledger technology, decentralized governance, non-custodial architecture, or automated execution, where the person exercises control, administration, governance, operational authority, fee extraction, front-end access, upgrade authority, or other material influence over the service."

5. Clarify authority over mixers and anonymizing services

After Van Loon, Congress should clarify the scope of sanctions and AML authority over digital asset mixers, anonymizing services, and obfuscation infrastructure. The goal should be targeted authority against laundering services, not a broad attack on privacy-enhancing technology or software publication.

Illustrative language: "The Secretary may designate or impose special measures on any digital asset mixer, anonymizing service, obfuscation service, or substantially similar service where the Secretary determines, based on substantial evidence, that the service is used to facilitate money laundering, terrorist financing, proliferation financing, ransomware, sanctions evasion, theft, fraud, trafficking, or the movement or concealment of corruption-related proceeds."

Illustrative safeguard: "In applying this authority, the Secretary shall consider as appropriate whether identifiable persons operate, administer, promote, profit from, control, or materially facilitate the service; the availability of lawful privacy-preserving use cases; and the feasibility of tailored measures that address illicit finance risk without unnecessarily restricting lawful activity."

6. Impose risk-based obligations for unhosted wallet exposure

Businesses that interact with unhosted wallets should have risk-based obligations when red flags are present, especially for large transfers, high-risk jurisdictions, sanctions exposure, mixers, fraud typologies, and corruption-related risk. FATF's 2026 stablecoin report specifically addresses misuse of stablecoins through unhosted wallets and peer-to-peer transactions.[xxxiii]

Illustrative language: "Covered digital asset intermediaries and permitted payment stablecoin issuers shall maintain risk-based controls for transactions involving unhosted wallets, including controls reasonably designed to identify and respond to sanctions exposure, illicit finance typologies, high-risk jurisdictions, mixers, darknet markets, terrorist financing, fraud, ransomware, trafficking, and corruption-related proceeds."

7. Require fraud prevention, preservation, and victim recovery

Crypto fraud moves quickly, but blockchain tracing can sometimes identify stolen funds before they are fully cashed out. Covered digital asset firms and stablecoin issuers should be required to maintain procedures to preserve and return traceable stolen assets when required by lawful process, including court orders for seizure, forfeiture, restitution, or victim return. Congress should also make clear that good-faith compliance with lawful process does not create undue liability.

8. Preserve sanctions authority and require operational sanctions compliance

Sanctions compliance in crypto cannot be theoretical. It requires screening, blockchain analytics, rapid response, issuer controls where available, escalation procedures, and coordination with law enforcement and OFAC. Stablecoin issuers and digital asset intermediaries should be required to demonstrate that they can identify and respond to sanctioned wallets, sanctioned platforms, and attempts to evade freezes or blocks.

Illustrative language: "Covered persons shall maintain sanctions compliance programs reasonably designed to identify, block, reject, freeze, or otherwise prevent prohibited transactions, including through screening of wallet addresses, counterparties, beneficial owners, geographic indicators, transaction patterns, and other risk indicators identified by the Secretary."

9. Strengthen information sharing and turn existing recommendations into action

Congress should not create new pilots, studies, or working groups that simply restate problems the government has already identified. Any information-sharing pilot should build on existing Section 314 authorities, include federal, state, and local law enforcement, and create feedback loops on whether suspicious activity reporting is actually useful. Any interagency process should focus on implementing existing Treasury, DOJ, and law-enforcement recommendations and identifying any remaining statutory text needed to close known gaps.

10. Fund enforcement and require public reporting

A statute is only as strong as the institutions implementing it. Congress should provide dedicated funding for FinCEN, OFAC, DOJ, IRS-CI, the FBI, and other relevant federal, state, and local law-enforcement partners to hire technologists, investigators, analysts, prosecutors, sanctions specialists, and victim-recovery personnel. It should also require Treasury to report regularly on digital asset illicit finance trends, enforcement gaps, and the effectiveness of the statutory framework.

Illustrative language: "There are authorized to be appropriated such sums as may be necessary to support digital asset-related AML/CFT supervision, sanctions enforcement, blockchain analytics, law enforcement training, asset tracing, asset forfeiture, and public-private information sharing."

CONCLUSION

The United States should approach digital assets with neither panic nor wishful thinking. The basic principle is straightforward: financial activity should carry financial crime obligations that match the risk. If a product or service moves value like a financial intermediary, it should not escape responsibility because it uses new technology. If an issuer creates a dollar-like instrument used across global markets, it should help protect that instrument from abuse. If a platform serves U.S. customers or relies on U.S. markets, it should not be able to avoid U.S. law by operating offshore. If a protocol is controlled, administered, promoted, or monetized by identifiable people or entities, they should not be able to collect the upside while disclaiming responsibility for the risks. And if law enforcement is expected to follow the money, Congress must give it the tools, records, authorities, and resources to do so.

The choice before Congress is not innovation or enforcement. It is whether the next generation of financial infrastructure will be built with basic safeguards from the start, or whether the United States will repeat a familiar pattern: allow illicit actors to exploit gaps in shell companies, real estate, art, private investment vehicles, and other secrecy channels, then spend years trying to repair the damage.

A crypto bill that addresses stablecoins, DeFi businesses and interfaces, offshore platforms, mixers, unhosted-wallet risk, sanctions compliance, fraud prevention, victim recovery, recordkeeping, information sharing, rapid law-enforcement response, and enforcement resources would do more than provide regulatory clarity. It would create a real market structure law for the real world.

METHODOLOGICAL NOTE

This report relies primarily on official U.S. government, FATF, and court materials. The appendix is illustrative and should be read as a set of examples showing recurring risk patterns, not as an exhaustive catalog of crypto-related crime. Private-sector blockchain analytics figures from Chainalysis and TRM Labs are included only as attributed estimates and should not be characterized as official government findings. Where litigation or regulatory authority is contested, the draft describes the posture narrowly and avoids claiming more than the cited source supports. Any version of this report tied to a specific legislative vehicle should be checked against the latest bill text, because CLARITY Act and stablecoin implementation language remains subject to change as of July 2026.[xxxiv]

ABOUT TRANSPARENCY INTERNATIONAL U.S.

Transparency International U.S. (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.

For more information, reach out to Transparency International U.S. at info-us@us.transparency.org.

APPENDIX: ADDITIONAL EXAMPLES OF CRYPTO AND DEFI ABUSE

Sanctions Evasion and Hostile-State Finance

a. North Korea / Lazarus Group. Lazarus Group is repeatedly identified as the central state-backed crypto theft and laundering actor. It includes examples such as Ronin, Harmony Horizon Bridge, Atomic Wallet, WazirX, DMM Bitcoin, Radiant Capital, and Bybit.[xxxv] The point is that crypto theft and laundering are now part of North Korea's sanctions-evasion and weapons-financing toolkit.
b. Bybit. The 2025 Bybit hack is the largest single cryptocurrency theft in history, attributed by the FBI to North Korea's TraderTraitor/Lazarus activity.[xxxvi] It highlights supply-chain compromise, rapid laundering, bridges, mixers, Chinese-language OTC brokers, and limited asset freezing.
c. DPRK IT workers. North Korean IT worker infiltration of crypto and technology firms is a distinct vector from hacking. A crypto bill alone cannot solve this, but AML/CFT obligations, suspicious activity reporting, sanctions screening, and beneficial ownership controls help surface the networks that support it.
d. Russia. Garantex, Grinex, Cryptex, PM2BTC, no-KYC exchanges, and Russian-language cash-out infrastructure are major sanctions-evasion and laundering channels. This supports the importance of successor designations and infrastructure seizures when sanctioned platforms reconstitute.
e. Bitzlato and exchange off-ramps. Darknet market activity has been linked to exchange off-ramps, including Bitzlato and Garantex. Criminal marketplaces depend on financial infrastructure, and a market structure bill should target the money movement layer, not just the visible marketplace.
f. Operation SpecTor and continuing marketplace migration. Darknet markets remain resilient. Takedowns work, but successor platforms and user migration are persistent. This evidence supports sustained law-enforcement funding and international cooperation, not one-time enforcement bursts.

Market Manipulation, Wash Trading, Fraud, and Pump-and-Dump Schemes

Wash trading is a recurring crypto market-integrity problem, with examples involving exchange reporting, market makers, and allegedly manipulated trading volume. The policy lesson is that market structure rules must address both investor protection and AML, because manipulated markets generate proceeds that then move through the same laundering infrastructure.

a. Coinbase CFTC settlement. The CFTC's 2021 order involving Coinbase for reckless false, misleading, or inaccurate reporting and wash trading by a former employee is useful as an official enforcement example of market-data integrity risk.[xxxvii]
b. Binance-related allegations and resolution. This includes alleged wash trading issues and the separate DOJ/Treasury resolution for AML and sanctions violations.
c. Hydrogen / HYDRO. The HYDRO case is an example of crypto securities price manipulation involving wash trades and spoof trades, resulting in criminal convictions and sentences.

d. Operation Token Mirrors. This marked DOJ's first-ever criminal charges against financial services firms for crypto market manipulation and wash trading, in which the FBI created a token and company to expose the alleged schemes. It provides a concrete enforcement example for market-manipulation provisions.
e. Gotbit. Gotbit is an example of wash-trading services sold to token projects. This case supports prohibiting paid market manipulation and requiring strong market surveillance.
f. Centra Tech. Centra Tech is an example of early ICO-era fraud, false claims, celebrity-style promotion, and weak investor protection.[xxxviii] It is useful as evidence that crypto fraud risks are not only technical; they often involve ordinary misrepresentations wrapped in financial innovation language.
g. BitConnect and OneCoin. These are major Ponzi-style crypto fraud examples.[xxxix] They support the argument that promoters and platforms should not be able to hide behind labels when they are soliciting investment, moving value, or facilitating fraud proceeds.
h. Pump-and-dump examples: Squid Game token, EthereumMax, Save the Kids, Hawk Tuah, Meteora, and $LIBRA are examples of retail-facing token manipulation or alleged manipulation.

Money Laundering, Mixers, Chain-Hopping and No-KYC Exchanges

a. Sinbad.io and Blender.io. Sinbad shows how successor infrastructure can emerge after enforcement: after OFAC sanctioned Blender.io, Lazarus Group and other illicit actors turned to another Bitcoin mixer that served a similar laundering function. The Sinbad case also illustrates the value of coordinated law-enforcement action, including FBI, Dutch, and Finnish cooperation to seize servers and domains.[xl]
b. Garantex. Garantex is a central example of exchange-based laundering and sanctions evasion: a Russia-linked no-KYC exchange originally registered in Estonia, later operating from Russia, was sanctioned by OFAC in 2022, and disrupted in 2025 after continuing to process high-risk and illicit activity. Garantex shows that sanctions alone may not stop a platform protected by a non-cooperative jurisdiction unless they are paired with infrastructure seizure, wallet freezes, arrests, and successor-entity designations.[xli]
c. Operation Final Exchange. Germany's 2024 seizure of 47 Russian-language no-KYC exchange platforms shows the value of moving beyond single-platform enforcement and targeting the broader laundering ecosystem.[xlii]
d. Cryptex, PM2BTC, and other Russian money-laundering infrastructure. Russian-language no-KYC exchanges and related services are critical off-ramps for ransomware, darknet market, fraud, and sanctions-evasion proceeds. These examples show why a bill must cover platforms serving U.S. customers or U.S.-dollar rails even if the platform is nominally offshore.

Darknet Markets and Crypto-Enabled Criminal Marketplaces

a. Silk Road. Silk Road is the foundational darknet market case: Tor plus Bitcoin plus escrow plus vendor reputation created the basic template for modern online illicit markets. The case also produced major crypto forfeiture and tracing examples, including later Silk Road-related Bitcoin seizures.[xliii]
b. AlphaBay and Operation Bayonet. AlphaBay is a much larger successor marketplace, with Bitcoin, Monero, Ethereum, and Zcash used in transactions. Operation Bayonet, including the

covert law-enforcement control of Hansa Market, is used as a model for intelligence-led enforcement that exploits predictable criminal migration after takedowns.[xliv]

c. Hydra Market. Hydra was the dominant Russian-language darknet market before its 2022 seizure, with a dead-drop delivery model, in-house mixing, and cash-out services.[xlv] Hydra is important because it was not just a drug market; it functioned as broader criminal financial infrastructure used by ransomware groups, fraud actors, and other illicit networks.

---

[i] U.S. Department of the Treasury, Innovative Technologies to Counter Illicit Finance Involving Digital Assets, Report to Congress Pursuant to the GENIUS Act (Mar. 2026), https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.

[ii] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf; U.S. Department of the Treasury, Treasury Releases 2023 DeFi Illicit Finance Risk Assessment (Apr. 6, 2023), https://home.treasury.gov/news/press-releases/jy1391.

[iii] Financial Action Task Force, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf; Financial Action Task Force, Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions (Mar. 3, 2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.

[iv] Chainalysis, 2026 Crypto Crime Report Introduction (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction. Chainalysis figures are proprietary blockchain analytics estimates and should be treated as methodology-dependent estimates, not official government statistics.

[v] TRM Labs, 2026 Crypto Crime Report Key Insights: TRM Identifies Record USD 158 Billion in Illicit Crypto Flows in 2025, Reversing a Multi-year Decline (Jan. 10, 2026), https://www.trmlabs.com/resources/blog/2026-crypto-crime-report-key-insights-trm-identifies-record-usd-158-billion-in-illicit-crypto-flows-in-2025-reversing-a-multi-year-decline. TRM figures are proprietary blockchain analytics estimates and should be treated as methodology-dependent estimates, not official government statistics.

[vi] U.S. Department of Justice, Binance and CEO Plead Guilty to Federal Charges in $4B Resolution (Nov. 21, 2023), https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[vii] U.S. Department of the Treasury, U.S. Treasury Announces Largest Settlements in History with World's Largest Virtual Currency Exchange Binance for Violations of U.S. Anti-Money Laundering and Sanctions Laws (Nov. 21, 2023), https://home.treasury.gov/news/press-releases/jy1925.

[viii] FinCEN, FinCEN Issues Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Finance (Aug. 4, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-notice-use-convertible-virtual-currency-kiosks-scam-payments-and.

[ix] FinCEN, Financial Trend Analysis: Fentanyl-Related Illicit Finance: 2024 Threat Pattern & Trend Information (Apr. 2025), https://www.fincen.gov/sites/default/files/shared/FinCEN-FTA-Fentanyl.pdf; FinCEN, FinCEN Issues Analysis of Fentanyl-Related Threat Patterns and Trends in Bank Secrecy Act Data (Apr. 9, 2025), https://www.fincen.gov/news/news-releases/fincen-issues-analysis-fentanyl-related-threat-patterns-and-trends-bank-secrecy.

[x] U.S. Department of Justice, Global Disruption of Three Terror Finance Cyber-Enabled Campaigns (Aug. 13, 2020), https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

[xi] FinCEN, FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Assets by the Iranian Revolutionary Guard Corps-Qods Force and Its Proxies (May 11, 2026), https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf.

[xii] U.S. Department of the Treasury, Economic Fury Targets Iran's Largest Digital Asset Exchange for Terror Finance and Sanctions Evasion (June 2, 2026), https://home.treasury.gov/news/press-releases/sb0519.

[xiii] Financial Action Task Force, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

[xiv] Financial Action Task Force, Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions (Mar. 3, 2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.

[xv] U.S. Department of Justice, South Korean National and Hundreds of Others Charged Worldwide in Takedown of the Largest Darknet Child Pornography Website (Oct. 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.

[xvi] Chainalysis, Cryptocurrency Flows to Suspected Human Trafficking Services Surge 85% Year-over-Year (Feb. 12, 2026), https://www.chainalysis.com/blog/crypto-human-trafficking-2026/.

[xvii] Financial Action Task Force, Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions (Mar. 3, 2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.

[xviii] Chainalysis, 2026 Crypto Crime Report Introduction (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.

[xix] FinCEN and OFAC, Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism and Sanctions Requirements, 91 Fed. Reg. 14933 (Apr. 10, 2026), https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.

[xx] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[xxi] U.S. Department of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[xxii] U.S. Department of Justice, North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[xxiii] U.S. Department of Justice, Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya; U.S. Department of Justice, Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme (May 1, 2024), https://www.justice.gov/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme.

[xxiv] U.S. Department of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

[xxv] Van Loon v. Department of the Treasury, No. 23-50669 (5th Cir. Nov. 26, 2024), https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf.

[xxvi] U.S. Department of the Treasury, Tornado Cash Delisting (Mar. 21, 2025), https://home.treasury.gov/news/press-releases/sb0057.

[xxvii] FinCEN, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021), https://www.fincen.gov/news/news-releases/fincen-issues-first-national-amlcft-priorities-and-accompanying-statements.

[xxviii] FinCEN, FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Assets by the Iranian Revolutionary Guard Corps-Qods Force and Its Proxies (May 11, 2026), https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf.

[xxix] U.S. Department of the Treasury, Economic Fury Targets Iran's Largest Digital Asset Exchange for Terror Finance and Sanctions Evasion (June 2, 2026), https://home.treasury.gov/news/press-releases/sb0519.

[xxx] U.S. Department of Justice, Binance and CEO Plead Guilty to Federal Charges in $4B Resolution (Nov. 21, 2023), https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution; U.S. Department of the Treasury, Binance settlement announcement (Nov. 21, 2023), https://home.treasury.gov/news/press-releases/jy1925.

[xxxi] FinCEN and OFAC, Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism and Sanctions Requirements, 91 Fed. Reg. 14933 (Apr. 10, 2026), https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.

[xxxii] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[xxxiii] Financial Action Task Force, Targeted Report on Stablecoins and Unhosted Wallets: Peer-to-Peer Transactions (Mar. 3, 2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf.

[xxxiv] Reuters, US Senate committee advances crypto bill in milestone for digital assets (May 14, 2026), https://www.reuters.com/legal/transactional/us-senate-committee-weigh-crypto-bill-milestone-digital-assets-2026-05-14/; U.S. Senate Committee on Banking, Housing, and Urban Affairs, Myth vs. Fact: The CLARITY Act (Jan. 13, 2026), https://www.banking.senate.gov/newsroom/majority/myth-vs-fact-the-clarity-act.

[xxxv] FBI, North Korea Responsible for $1.5 Billion Bybit Hack (IC3 PSA 250226, Feb. 26, 2025), https://www.ic3.gov/PSA/2025/PSA250226; U.S. Department of the Treasury, DPRK-related cyber and virtual asset theft sanctions materials.

[xxxvi] FBI, North Korea Responsible for $1.5 Billion Bybit Hack (IC3 PSA 250226, Feb. 26, 2025), https://www.ic3.gov/PSA/2025/PSA250226; Chainalysis, TRM Labs, and Elliptic public analyses of the Bybit laundering flows.

[xxxvii] Commodity Futures Trading Commission, Coinbase Inc. order regarding reckless false, misleading, or inaccurate reporting and wash trading (Mar. 19, 2021), https://www.cftc.gov/PressRoom/PressReleases/8369-21; U.S. Department of Justice, First-ever criminal charges against financial services firms for cryptocurrency market manipulation and wash trading (Oct. 9, 2024), https://www.justice.gov/opa/pr/18-individuals-and-entities-charged-international-operation-targeting-widespread-fraud-and.

[xxxviii] U.S. Department of Justice, Founders of Cryptocurrency Company Indicted in Manhattan Federal Court With Scheme to Defraud Investors (May 12, 2018), https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-company-indicted-manhattan-federal-court-scheme-defraud; SEC, SEC Charges Additional Defendant in Fraudulent ICO Scheme (Apr. 20, 2018), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-24117.

[xxxix] U.S. Department of Justice, Founder of Fraudulent Cryptocurrency Charged in $2 Billion BitConnect Ponzi Scheme (Feb. 25, 2022), https://www.justice.gov/usao-sdca/pr/founder-fraudulent-cryptocurrency-charged-2-billion-bitconnect-ponzi-scheme; U.S. Department of Justice, Co-Founder of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison (Sep. 12, 2023), https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison.

[xl] U.S. Department of the Treasury, Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency (Nov. 29, 2023), https://home.treasury.gov/news/press-releases/jy1942; U.S. Department of Justice, Operators of Cryptocurrency Mixers Charged with Money Laundering (Jan. 10, 2025), https://www.justice.gov/opa/pr/operators-cryptocurrency-mixers-charged-money-laundering.

[xli] U.S. Department of Justice, Garantex Cryptocurrency Exchange Disrupted in International Operation (Mar. 7, 2025), https://www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation; U.S. Department of the

Treasury, Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals (Aug. 14, 2025), https://home.treasury.gov/news/press-releases/sb0229.

[xlii] Chainalysis, In Large Operation, German Law Enforcement Seizes Servers of 47 Russia-centric No KYC Exchanges (Sep. 25, 2024), https://www.chainalysis.com/blog/german-authorities-seize-russia-centric-exchanges/.

[xliii] U.S. Department of Justice, U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud (Nov. 7, 2022), https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction.

[xliv] U.S. Department of Justice, AlphaBay, the Largest Online Dark Market, Shut Down (July 20, 2017), https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down; Europol, Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation (July 20, 2017), https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[xlv] U.S. Department of Justice, Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace (Apr. 5, 2022), https://www.justice.gov/usao-ndca/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace; U.S. Department of the Treasury, Treasury Sanctions Russia-Based Hydra Market and Virtual Currency Exchange Garantex (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701.