

NATIONAL SHERIFFS' ASSOCIATION



July 31, 2026

The Honorable John Thune
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Charles Schumer
Minority Leader
United States Senate
Washington, D.C. 20510

Dear Majority Leader Thune and Minority Leader Schumer:

On behalf of the National Sheriffs' Association (NSA), representing 3,081 sheriffs and approximately 10,000 public safety professionals, including deputies, investigators, and other sworn and civilian law enforcement personnel across the United States, we are sharing the attached memorandum to ensure you have a clear understanding of where the nation's sheriffs stand, and what our serious concerns are, with respect to the CLARITY Act.

While NSA supports establishing a responsible regulatory framework for the digital-asset marketplace, the legislation's significant law enforcement and public safety risks must be addressed before the Senate votes. Of particular concern, the bill would create broad exemptions from registration, know-your-customer, anti-money-laundering, and sanctions-law requirements for certain decentralized-finance participants, potentially allowing illicit actors to exploit platforms and services designed to obscure digital-asset transactions. By removing these foundational safeguards, the bill would make it harder to prevent financial crimes before they occur, impede law enforcement's ability to investigate and disrupt criminal networks, and reduce opportunities to recover stolen assets and protect victims.

The attached memorandum provides a section-by-section analysis of the harmful legislation, explains NSA's concerns with key provisions, and offers recommendations and proposed legislative changes to address them. We urge the risks of this bill be addressed before the Senate votes.

NSA stands ready to discuss these issues.

Sincerely,


Sheriff Troy Wellman
Moody County, SD
President
National Sheriffs' Association


Justin Smith
Executive Director, CEO
National Sheriffs' Association

Attachment: Regulating the Digital-Asset Marketplace and CLARITY

cc: U.S. Senate



NATIONAL SHERIFFS' ASSOCIATION

July 29, 2026

Regulating the Digital-Asset Marketplace and CLARITY

1. **Background.** In July 2025, Congress enacted the **GENIUS Act** and regulated issuers of stablecoins.¹ *Now*, Congress should regulate the digital-asset **marketplace** through which all types of digital assets—including stablecoins, cryptocurrencies, and privacy coins—move through the financial system. Broadly speaking, marketplace participants fall into two groups: (1) those that are, or work like, traditional financial institutions, and (2) those that use new technology and software (*e.g.*, blockchain technology and smart contracts) to enable persons to do things, like make payments or send money, in largely automated ways. Both groups involve risks of money laundering and financing terrorism or proliferation.²

2. **Regulate Everyone.** Congress should regulate *all* participants in the marketplace according to their activities and risks. No class of participants should receive a blanket exemption from registration, know-your-customer (KYC), anti-money laundering (AML), and sanctions-law obligations.

3. **Digital-Asset Service Providers.** In its early efforts to identify the persons and entities to regulate for AML and CFT risk, the Financial Action Task Force (FATF)³ defined a **virtual-asset service provider** and recommended that gov'ts require all of them to have AML policies and practices consistent with their activities and risk. FATF's Recommendations 15 and 16 are key here.

<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>

In GENIUS, Congress patterned the definition of **digital-asset service provider** on FATF's definition. *See* 12 U.S.C. § 5901(7). But GENIUS attached no real AML or other duties *to* digital-asset service providers. Congress should do this *now*.

The Future. As various illicit-finance risks—such as those associated with stablecoins, unhosted wallets, and other new developments—emerge and grow,⁴ gov'ts will regulate *all* persons and businesses with the right relationship to the digital-asset marketplace; that is, everyone who receives revenue from it.⁵

4. **New Technology & New Systems or Platforms.** Some want to set up a special kind of computer system in which users can send digital assets to other users, or pay for goods or services, using the system. The user at each end of a transaction stores his or her digital assets, such as a digital currency, in his or her own **wallet**. The sender or buyer accesses a **digital-asset services platform**—often through a friendly, easy-to-use graphical interface called a **front-end** on a phone or laptop—and gives an instruction to send a specific amount of a digital asset to the recipient's or seller's wallet. When it receives the sender's or buyer's instructions, a **smart contract** self-executes the instruction and sends the digital asset to the other's wallet.

Blockchain technology makes such a system possible. A blockchain accurately encodes transaction information—such as the sender, the recipient, amount, and dates—on the chain itself. As more transactions occur, they are recorded on the blockchain. In most cases, the blockchain is **public**, and this is an important feature. This allows anyone to check a blockchain and **verify** the recorded transactions and, thus, their *value*. This is why people participate and use the technology.

Significantly, the system—a digital-asset services platform—would not necessarily involve a bank or traditional financial institution, and it *wouldn't necessarily exist in one central place*. Also, in some platforms, one person or one group acting together would *not govern* the system. Instead, the underlying computer programs, including smart contracts, and governance or decision-making would be spread across communities of users. Some of the smart contracts would be immutable.

To be clear, some can and will set up these new systems—digital-asset services platforms—and run them responsibly. That is, they will retain the ability to screen and verify users, give users helpful information and warnings about scams on their front-ends, monitor for suspicious financial activity and report it, cooperate with law enforcement to fight crime and help victims (*e.g.*, by freezing transactions on request), and generally perform various AML functions.

Others, however, will not and do not. They want to set up fully **decentralized** digital financial services platforms that transfer digital assets (or facilitate transfers) with *only* the individual users—senders and buyers; recipients and sellers—giving instructions. CLARITY's authors want to **exempt** these decentralized marketplace participants from AML/CFT regulation, even though they know bad actors will use them.

5. DeFi and Mixers & Tumblers. After its May 14, 2026 markup, Senate Banking released a 594-page text of CLARITY, and, on July 22, 2026, Senate Banking and Senate Agriculture released a 616-page text.⁶ Contrary to good policy, the bill's authors want to create a **blanket exemption** for decentralized finance protocols (**DeFi**), including non-controlling developers and providers or, alternatively named, non-controlling blockchain developers and non-controlling providers of blockchain services. This exemption would include platforms set up by actors who do not like the public nature of most blockchains, such as mixers, tumblers, cross-chain bridges, and similar transaction-obfuscating services. Such an exemption would be poor policy.

6. Section 10201. CLARITY has 12 titles that address aspects of the digital-asset marketplace, and title 2 addresses protecting against illicit finance. Because of its position at the top of the statute, section 10201 *should* impose AML obligations on *all* participants in the marketplace. But it wouldn't. Instead, it would impose AML duties on only a digital-commodities broker, a digital-commodities dealer, and a digital-commodities exchange (*e.g.*, 134:5–136:8). As written, section 10201 would impose new AML duties on practically *no one* and would **increase** confusion regarding which digital-asset businesses have AML responsibilities under the current patchwork of regulation and law.⁷ Congress should fix this. For example, Congress could add a definition of digital-asset service provider (the FATF global standard definition, similar to the one GENIUS references) to the current definition of financial institution at 31 U.S.C. § 5312(a)(2).⁸ This would clearly put all participants under the AML and sanctions-law regulations that currently apply to banks and other financial institutions.

7. Section 10301. CLARITY's title 3 addresses decentralized finance, and section 10301 is a big exemption. Section 10301 would exempt decentralized finance trading protocols from AML requirements, including those that apply to registration, conduct, disclosure, recordkeeping, supervision, and other requirements (*e.g.*, 166:10–168:17; 169:6–20). Treasury has already reported on the risks presented by DeFi, stating, “This risk assessment explores how illicit actors are **abusing** what is commonly referred to as decentralized finance (DeFi) services as well as vulnerabilities unique to DeFi services.”⁹ No good reason supports exempting entire classes of marketplace participants.

In 2026, Treasury discussed DeFi's role in ransomware schemes, digital-asset service providers' attempts to evade AML practices, and the current regulatory framework's difficulties in controlling illicit-finance risks in decentralized protocols where governance or decision-making is distributed across communities of users and where the protocols may be immutable. *See* Treasury, 2026 National Money Laundering Risk Assessment, at 21–22, 50–51, 54, <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>.

CLARITY should meaningfully *regulate* DeFi, not give DeFi participants a blanket exemption from AML obligations appropriate for their activities and risks.¹⁰ For example, Congress could require Treasury to issue rules to apply BSA obligations to a covered business that (1) isn't otherwise a BSA-covered entity, (2) derives at least \$1 million per year in relation to a certain decentralized financial services platform, (3) has a purpose to increase customers, traffic, or transactions on the platform, (4) has employees, and (5) has the ability to propose updates or modifications to the platform or had a significant role in developing or operating the platform. Businesses who meet these criteria can afford to register and implement AML.

8. **Section 10604.** In the May 14, 2026 and earlier versions of CLARITY, section 604 would have specially exempted so-called non-controlling developers or providers (310:3–11) from registration and AML requirements that would apply to money-transmitting businesses, such as those in 31 U.S.C. § 5330 and 18 U.S.C. § 1960 (*e.g.*, 310:12–311:12).¹¹ Along with section 10301, section 10604 would have exempted mixers, tumblers, and cross-chain bridges from AML obligations, despite the fact that their sole purpose is to obfuscate transaction trails and movements of digital assets and impair law enforcement's ability to fight crime and recover victims' assets.

See Treasury, Illicit Finance Risk Assessment of Decentralized Finance, at 10 (2023) (“Decentralized Mixers functionally obfuscate the source, destination, or amount involved in a virtual asset transaction. These types of services may involve centralized or decentralized mechanisms and may be effectuated using several techniques.”), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>.

Many protested.

Around July 7, 2026, Senate Banking circulated a proposal to *strengthen* section 604's exemption for non-controlling blockchain developers or providers of a blockchain service. On July 22, 2026, Senate Banking and Senate Agriculture proposed to restore the May 14 text of section 10604 (in May 14, section 604).

Both the July 7 and July 22 versions would be terrible policy.¹² Congress should delete section 10604. Alternatively, Congress should fix it by adopting Senator Catherine Cortez Masto's proposal to exclude certain software developers and providers from 10604's exemption based on various factors (*e.g.*, custody of users' assets, ability to transact, participation in an operation to facilitate digital-asset transfers between others, and compensation). Congress could also narrow 10604's exemption to include only the least risky types of software developers, such as operators of oracles, node providers, and some data suppliers, as listed in the White House's 2025 *Strengthening American Leadership in Digital Financial Technology*, <https://www.whitehouse.gov/wp-content/uploads/2025/07/digital-Assets-Report-EO14178.pdf>.

9. **Section 10302.** Section 10302 would direct Treasury to issue *guidance* to front-ends on how to take AML and sanctions-law steps (176:17–179:13). But people who are not tech savvy access the digital-asset marketplace through easy-to-use **front-ends** or graphical interfaces (which may be on a phone app or on a website),¹³ and those front-ends are a great juncture to impose KYC and AML obligations, such as verifying

users and monitoring for suspicious activity and reporting it to law enforcement. Also, regulatory-technology (RegTech) services show that front-ends can already perform valuable and effective AML functions.¹⁴ Thus, guidance is insufficient. Congress should require all front-ends with a connection to the digital-asset marketplace to perform risk-based KYC/AML functions.

In addition to the fact that it would require Treasury to issue only non-binding guidance, section 10302 would also freeze Treasury in time. Section 10302 would authorize Treasury to issue guidance on how to comply with only *existing* AML and sanctions laws with no authority to keep up with the market or bad actors (*e.g.*, 179:20–180:20). This makes no sense in a rapidly developing field such as digital assets.

10. Section 10303. U.S. sanctions law—enforced primarily by the Depts. of Treasury (Office of Foreign Assets Control (OFAC)), State, and Commerce—is a set of measures that allow an agency, such as OFAC, to identify suspicious persons and organizations and put them on a sanctions list. In general, U.S. law prohibits or severely restricts the ability of *all* U.S. persons and persons subject to U.S. jurisdiction from doing business with a person or entity on a sanctions list.¹⁵

In a 2024 opinion, however, the U.S. Court of Appeals for the Fifth Circuit held that a key U.S. sanctions statute, the International Emergency Economic Powers Act (IEEPA), reaches, in relevant part, only *property* and that Treasury cannot sanction Tornado Cash, a notorious mixing platform, because immutable smart contracts—a key piece of technology in DeFi (a smart contract can self-execute various actions, such as a digital-asset transaction, upon receipt of a qualifying instruction¹⁶)—are *not* property. The court invited Congress to update IEEPA to target new technology such as “crypto-mixing technology.” *Van Loon v. U.S. Dept. of Treasury*, 122 F.4th 549 (5th Cir. 2024).¹⁷

CLARITY should do just that. That is, Congress should authorize Treasury to sanction all persons in, and components of, the digital-asset marketplace, including smart contracts and everything else in the ecosystem, and then to prohibit or restrict all U.S. persons dealing with persons or entities on a sanctions list.

Section 10303 would *not* do that. Section 303 would extend limited authority to reach transactions involving only domestic financial institutions or agencies—but not all marketplace participants. For example, any U.S. person with a wallet would be free to continue transacting with high-risk DeFi service providers, even if Treasury targeted them. It would not amend IEEPA or otherwise restore Treasury’s ability to sanction any platform in the digital-asset marketplace, even one that repeatedly facilitated illicit activity.

11. Section 10205. Section 10205’s purpose is to rein in the abuses of crypto-ATMs or kiosks. Scammers love to steer elderly victims to these kiosks and have them buy crypto-currency with cash or their credit or debit cards. Scammers then launder the digital currency through mixers, tumblers, or similar services.

First, section 10205 was patterned on Sen. Richard Durbin’s bill, S. 710, the Crypto-ATM Fraud Prevention Act,¹⁸ which law enforcement generally supported. But section 10205 deleted the provision that imposed a duty to detect and prevent fraud, and section 10205 weakened S. 710’s provisions that required real refunds to defrauded or scammed customers.

Second, in the May 14 CLARITY text, section 205 substituted a provision to prohibit a digital-asset kiosk operator from executing a new customer’s transaction until at least 72 hours have elapsed after the customer initiated the transaction (*e.g.*, 398:20; 402:13–17; 408:13–17). But 205 wouldn’t have conferred a right for

the customer to *cancel* a transaction within those 72 hours. So, law enforcement asked the drafters to add a right to cancel within 72 hours and a provision to require a kiosk operator to refund a customer's money (the transaction amount *and* all fees) for failure to cancel a transaction after receiving a timely instruction to cancel.

In the July 22 CLARITY text, the authors—as their chief concession to law enforcement—*improved* section 10205 by adding a right to cancel and a refund provision (150:16; 160:19–161:21).

12. Section 10305. Section 10305 would shield a digital-asset service provider who voluntarily complies with a law-enforcement request to suspend a suspicious transaction temporarily from civil liability. Although some think section 10305 is great, it is voluntary. Moreover, it is special treatment for cooperating digital-asset service providers. For comparison, banks and other traditional financial institutions face this lawsuit risk with no liability shield when they cooperate with law-enforcement requests.

13. Law-Enforcement Provisions. Title 9 would provide some tools to assist law enforcement. But title 9 wouldn't make up for the exclusion of DeFi service platforms and participants from registration, AML, and sanctions-law obligations. CLARITY's proponents tout sections 10202, 10307(b), 10307(d), and 10303 as strengthening law enforcement.¹⁹ These provisions would require Treasury to develop examination standards to assess *financial institutions* involved in digital-asset transactions for AML/CFT compliance, ensure *financial institutions'* reporting includes digital-asset transactions for the sake of "law enforcement's ability to investigate, trace, and seize illicit digital asset flows," require Treasury to issue guidance for *financial institutions* "that engage with self-hosted wallets," and authorize Treasury to use sanctions authority against U.S. *financial institutions* who deal with a person or entity on a sanctions list. Thus, these proponents *recognize these risks and the related AML measures*, and they nonetheless want to exempt DeFi actors—who won't meet the definition of "financial institution"—from comparable regulations.²⁰

14. Rulemaking Authority & The Future. CLARITY would try to freeze regulatory, enforcement, and prosecutorial authority in time. For example, sections 10109, 10301, 10302, and 10604 would try to freeze aspects of Treasury's, CFTC's, or SEC's regulatory authority over some digital-asset service providers, including specifically mixers, tumblers, and similar service providers.²¹ Not only should it reject this, but Congress should clearly commit the tasks of studying, reporting on, and regulating the digital-asset marketplace and all participants to the appropriate agencies. And Congress should authorize them to issue emergency and temporary regulations to fight money laundering and other crime in this developing area (much like the DEA's authority to make emergency and temporary scheduling decisions to keep pace with the illicit drug trade). Congress should restore Treasury's full sanctions authority.

15. The Policy Decision. The key policy decision is whether Congress *should* create this extreme DeFi exemption. As written, CLARITY would create a world where criminals and foreign antagonists are free to use unregistered, nearly autonomous DeFi financial-services platforms with no AML functions to transfer and launder money in the form of digital assets. The platforms won't be *fully* autonomous, however, because they will act to ensure that the people with the right relationship to the platform are enriched by their operations. Also, DeFi's current organization creates risk of "fraud, rug-pulls, and other actions by project developers and programmers" and coding errors in smart contracts may allow "hackers to manipulate token prices, steal funds, or drain investors' crypto holdings"²² A blanket exemption would be poor policy. The National Sheriffs' Association is willing to offer and discuss bill text.

Endnotes

¹ **GENIUS.** See GENIUS Act, Pub. L. No. 119-27, 139 Stat. 419 (July 18, 2025) (codified at 12 U.S.C. §§ 5901–5916) (S 1582); Seth C. Oranburg, The GENIUS Dilemma: Innovation versus Antifraud in Stablecoin Regulation, 9 Stanford J. of Blockchain Law & Policy 1 (Jan. 4, 2026) (“Yet [this article] reveals latent tensions, including potential jurisdictional overlaps and diluted antifraud measures, that require rapid rulemaking and interagency coordination to avert persistent issuers. Moreover, GENIUS may not apply to state-issue stablecoins, creating a different regime for private issue[r]s and state actors.”), <https://stanford-jblp.pubpub.org/pub/genius-dilemma/release/1>; Arthur E. Wilmarth, Jr., “The Looming Threat of Uninsured Nonbank Stablecoins,” 50 Del. J. of Corp. L. 3, 8 (2025) (“[T]he GENIUS Act would greatly increase the likelihood that future runs on stablecoins would cause systemic financial crises and require massive government bailouts.”), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5272859.

² **Digital-Asset Risks.** See, e.g., Treasury, 2026 National Money Laundering Risk Assessment, at 21–22, 50–51, 54 (discussing the money-laundering risks of decentralized financial services), <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>; ; H.R. Rep. No. 119-612, Part 1, at 3 (Apr. 15, 2026) (“[T]ransnational criminal organizations are increasingly using new financial systems, like digital assets as part of criminal schemes, to include ransomware, fraud, and money laundering. Significant aspects of this illicit activity involve unlicensed money transmitting businesses, the illicit structuring of transactions, and other criminal or unlawful activity in or against organizations that are not federally insured financial institutions, but are financial institutions as defined under the Bank Secrecy Act. The gaps between existing U.S. law and contemporary criminal activity presents substantial challenges for U.S. law enforcement in addressing new forms of criminal activity involving digital assets.”), <https://www.congress.gov/119/crpt/hrpt612/CRPT-119hrpt612.pdf>.

The former Co-President of Harvard Law School Blockchain & FinTech Initiative wrote:

“But several features of cryptocurrencies still make them uniquely appealing for money laundering purposes.

First, cryptocurrencies allow cross-border transfers of money-like value without the aid of central intermediaries and the compliance requirements typically associated with the movement of fiat money through the international banking system, especially if self-hosted wallets and decentralized exchanges are used.

Second, cryptocurrency transactions can be settled in minutes; there is no cap on the value of cryptocurrency that can be transferred in a transaction, allowing launderers to quickly transfer large value; transactions in cryptocurrencies, moreover, are irreversible. While there is a risk of price fluctuation during the process of transfer, transfer of cryptocurrencies to jurisdictions where anti-money laundering regulations are lax can facilitate the process of exchanging cryptocurrencies back to fiat money or more stable assets at opportune moments, thus reducing the exposure to volatility risks.

Furthermore, cryptocurrencies are an ideal transaction medium for cybercriminals, such as ransomware hackers and scammers, who now increasingly demand payment in Bitcoin or Ether than in cash. Indeed, the FBI’s Internet Crime Report indicated that losses from crypto investment scams in the U.S increased more than 45% to \$3.94 billion in 2023; while payments from crypto-related ransom attacks nearly doubled to a record of \$1 billion in 2023. The draws of cryptocurrencies are obvious in these contexts. Multiple crypto wallet addresses can be created without identity verification, giving criminals a certain degree of anonymity. Moreover, the process of receiving crime proceeds in cryptocurrencies and that of laundering those proceeds can be automated, making the operations easier for technology-savvy cybercriminals.”

Heather Yue Zhou, Regulating Crypto Money Laundering: An Assessment of Current Regulatory Responses and Potentials for Technology-Based Solutions, 8.2 Stanford J. of Blockchain L. & Pol’y 142, 146 (June 30, 2025) (notes removed), <https://stanford-jblp.pubpub.org/pub/crypto-laundering/release/1>.

³ **G7 & FATF.** The G7 is an intergovernmental political and economic forum, and its members are Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. *See* G7 Italia, “About the G7” (visited July 15, 2026), <https://www.g7italy.it/en/about-g7/>. The G7 founded the Financial Action Task Force (FATF) in 1989, and the FATF issues policy and standards to fight money laundering and the financing of terrorism and proliferation. *See* U.S. Dept. of Treasury, “Financial Action Task Force” (visited July 15, 2026), <https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/financial-action-task-force>. Although it publishes various papers, such as targeted reports, FATF’s most important and influential publication is its Recommendations. *See* FATF, “What we do” (visited July 15, 2026), <https://www.fatf-gafi.org/en/the-fatf/what-we-do.html>; FATF Recommendations, <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/fatf-recommendations-2012.pdf>.

⁴ **New Risks.** As examples, FATF reports:

“2. Stablecoins, including through unhosted wallets, have become a common component of ML, TF, and PF schemes that use virtual assets. * * * Reporting indicates that stablecoins are the most popular virtual asset used in illicit transactions.

3. P2P transactions via unhosted wallets represent a key vulnerability in the stablecoin ecosystem. Conducted without the involvement of AML/CFT-obligated intermediaries, these transactions can be of higher risk, especially when layered through unhosted wallets.

* * *

31. While the specific techniques may differ by crime or group, common themes include use of unlicensed or unregistered VASPs, which are often located in jurisdictions without AML-CFT controls for VASPs, or VASPs that fail to comply with AML/CFT obligations, often over the counter (OTC) brokers or peer-to-peer platforms. Threat actors also use obfuscation techniques and services, like mixers and chain hopping. Stablecoins are used at various points in a longer transaction process, including being received as proceeds from the predicate crime or in the last leg to convert illicit virtual assets into fiat currency.

* * *

50. To address this gap, the FATF Guidance for a Risk-Based Approach to VAs and VASPs makes clear that VASPs should collect the required originator and beneficiary information even when conducting a transfer between their customer and an unhosted wallet. Jurisdictions that allow VASPs to undertake transfers with unhosted wallets should assess the risks and implement commensurate risk mitigation measures.”

FATF, Targeted Report on Stablecoins and Unhosted Wallets (Peer-to-Peer Transactions), at 3, 12, 19 (Mar. 2026), <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf>; *see* United Nations, “Money laundering through cryptocurrencies,” UN Toolkit on Synthetic Drugs (visited July 28, 2026) (discussing the money-laundering risks of privacy coins and mixers—including their role in obfuscating transaction trails—and urging member states to “introduce proper regulation and supervision of cryptocurrency markets”), <https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/laundryingproceeds/moneylaundering.html>; TRM Team, “Understanding the Use of Cryptocurrencies by Cartels,” TRM Labs (Jan. 21, 2025) (“Cryptocurrencies—with their unique ability to enable rapid, cross-border, and pseudonymous financial transactions—are increasingly being leveraged by transnational criminal organizations, including Mexican drug cartels. Among the most notorious of these groups, the Sinaloa Cartel has experimented with digital assets to launder proceeds from its lucrative drug trafficking operations.”), <https://www.trmlabs.com/resources/blog/understanding-the-use-of-cryptocurrencies-by-cartels>; UNODC, World Drug Report: Highlights, at 57 (2026) (“Delivery of the drugs is usually done by public or private postal services and payment is conducted by way of cryptocurrencies. Historically, the predominant currency for such transactions was Bitcoin, but recent years have seen the growing use of ‘privacy coins’ (such as Monero) specifically engineered to avoid the traceability and transparency of Bitcoin’s public ledger. According to some reports, Monero may have already started to outperform Bitcoin on darknet markets.”), <https://www.unodc.org/documents/data-and->

[analysis/WDR_2026/WDR26_Highlights.pdf](#); CFTC, Prediction Markets; Public Interest Determinations, 91 Fed. Reg. 35,806 (June 12, 2026) (proposing new rules to regulate prediction markets and event contract derivatives).

⁵ **Regulate Digital-Asset Beneficiaries.** *See, e.g.*, S. 2669, Digital Asset Anti-Money Laundering Act of 2023, 118th Cong. (2023) (proposing, in part, to add unhosted-wallet service providers to the BSA’s list of financial institutions at 31 U.S.C. §5312(a)(2)); Kuzi Charamba, Yan Yue Joyce Shum, & Douglas W. Arner, “Building Castles in the Sky? The Myth of Decentralized Finance and the Necessity of Legal Ordering, 25 Wash. U. Global Stud. L. Rev. 1, 15 (2025) (“The pressing need for an international consensus on an appropriate regulatory approach for DeFi has prompted global financial standard-setting organizations to issue relevant guidelines for major economies to consider.”), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5796883.

⁶ **Senate Banking & Agriculture’s July 22, 2026 Text**, <https://www.lummis.senate.gov/wp-content/uploads/Clarity-Act.pdf>; **Banking’s May 14 Text**, <https://www.congress.gov/119/bills/hr3633/BILLS-119hr3633rs.pdf>.

⁷ **Confusion about AML Obligations.** *See, e.g.*, Treasury, 2026 National Money Laundering Risk Assessment, at 51 (“Some digital asset service providers, including purportedly decentralized finance (DeFi) services or P2P platforms, may claim not to be regulated financial institutions subject to the BSA. Determining whether an entity, including purported DeFi services, is a covered financial institution will depend on specific facts and circumstances surrounding its financial activities.”), <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>; *id.* at 54 (“Relatedly, some DeFi services may fall outside of the AML/CFT framework in the United States and, as such, may not implement measures to mitigate illicit finance risk. Such instances can present a vulnerability, although these transactions may occur on public blockchains providing some transparency.”); Mollie Rouan, Note, Show Me the Money: Approaches to Anti-Money Laundering Compliance for Digital Assets, 19 Brooklyn J. of Corp., Financial & Commercial Law 485, 487 (2024) (“Currently, the US has adopted the approach of identifying ‘the legal status of crypto assets and applying the rules governing financial instruments with similar legal status.’ While this may be a straightforward approach to addressing a regulatory gap, ‘this method causes various authorities to apply unharmonized interpretations and standards simultaneously, reducing the industry’s regulatory efficiency.’ Alternatively, the MiCA regulation [The EU’s Markets in Crypto-Assets (MiCA) regulation] establishes a cohesive regulatory framework regarding the legal status of digital assets. In so doing, digital asset firms can rely on a consistent and predictable application of the MiCA regulation. This will likely lead to increased investor protection and more clarity for firms to achieve compliance.”), <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1454&context=bjcfcl>.

⁸ **Definition of a DASP.** The Financial Action Task Force (FATF) defines a **virtual-asset service provider (VASP)** as “any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- i. exchange between virtual assets and fiat currencies;
- ii. exchange between one or more forms of virtual assets;
- iii. transfer of virtual asset;
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- v. participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.”

FATF, The FATF Recommendations, International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation, at 140–141 (updated June 2026), <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/fatf-recommendations-2012.pdf>.

In the GENIUS Act, Congress patterned its definition of **digital-asset service provider (DASP)** on FATF’s definition. *See* 12 U.S.C. § 5901(7). But GENIUS exempted distributed-ledger protocols, the business of developing distributed-ledger protocols or self-custodial software interfaces (wallets), immutable and self-custodial software interfaces, transaction validators, and participation in liquidity pools for P2P transactions from the definition of a DASP. *See id.*

§ 5901(7)(B). CLARITY should repeal subsection 5901(7)(B) because regulations that require the embedding of AML measures into code should reach these service providers.

⁹ **DeFi Risks.** Treasury, Illicit Finance Risk Assessment of Decentralized Finance, at 1 (2023) (“This risk assessment explores how illicit actors are abusing what is commonly referred to as decentralized finance (DeFi) services as well as vulnerabilities unique to DeFi services. The findings will inform efforts to identify and address potential gaps in the United States’ anti-money laundering and countering the financing of terrorism (AML/CFT) regulatory, supervisory, and enforcement regimes for DeFi.”) (emphasis added), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>; ONDCP, Nat’l Drug Control Strategy, at 37 (2026) (“We will relentlessly pursue and dismantle drug trafficking networks wherever they operate. This includes attacking criminal exploitation of . . . digital payment platforms . . .”), <https://www.whitehouse.gov/releases/2026/05/2026-national-drug-control-strategy-released/>; Caroline Greenwell & Bella Henry, Charles Russell Speechlys, Expert Insights, “AML in decentralized finance and traditional finance” (Feb. 4, 2025) (“DeFi’s borderless transactions and anonymity pose significant regulatory challenges. Despite increased regulation on virtual asset service providers, the peer-to-peer nature of DeFi allows criminals to quickly replicate systems applying further regulation with new DeFi services, thereby thwarting AML protections. Hallmarks of DeFi, such as privacy and lack of centralised control, make it difficult to track and trace transactions back to their source, creating a major roadblock for authorities in detecting and preventing money laundering.”), <https://www.charlesrussellspeechlys.com/en/insights/expert-insights/dispute-resolution/2025/aml-in-decentralized-finance-and-traditional-finance/>.

¹⁰ **Practicality of Regulating DeFi.** *See, e.g.,* Gina-Gail S. Fletcher, Veronica Root Martinez, & Steven L. Schwarcz, Regulating DeFi Platforms, 111 Minn. L. Rev. _ (2026) (forthcoming) (“This Article argues that because DeFi platforms disaggregate traditional intermediary functions, effective regulation must focus on (i) embedding compliance safeguards directly into platform design and (ii) holding accountable the actors who build, operate, and maintain those platforms. These safeguards are essential to preserve market integrity, mitigate systemic risk, and protect investors in the absence of conventional intermediaries. Specifically, regulators should develop reforms that require platforms to incorporate technological and governance tools that replicate the critical compliance and risk-management functions historically supplied by intermediaries.”), <https://scholars.duke.edu/publication/1687611>; Kuzi Charamba, Yan Yue Joyce Shum, & Douglas W. Arner, “Building Castles in the Sky? The Myth of Decentralized Finance and the Necessity of Legal Ordering, 25 Wash. U. Global Stud. L. Rev. 1 (2025) (arguing that to be successful, true DeFi must rely on external legal ordering and enforcement or build its own standards and approaches to embedded regulation and supervision within its own systems), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5796883; *id.* at 6 (“Indeed, while DeFi protagonists may use technology to facilitate innovation in the operation of financial systems, this does not address the need for the provision of services for the administration of justice. This includes dispute resolution, policing and investigation, particularly in relation to fraud and criminal activities, and the protection of assets.”); Kai Wang, Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act, 4 U. Chicago Business L. Rev. 341 (2025) (arguing that “cryptocurrency non-custodial service providers, despite not taking custody of payment assets, can retain a certain degree of controlling power over payment assets in three key dimensions: (1) clearing and settlement, (2) asset ownership, custody, and balance sheet recording, and (3) governance” and that the BSA should cover some of these service providers), https://businesslawreview.uchicago.edu/sites/default/files/2025-10/Kai%20Wang_0.pdf; FATF, Targeted Report on Stablecoins and Unhosted Wallets (Peer-to-Peer Transactions), at 8 (Mar. 2026) (“Issuers [of stablecoins] can program smart contracts to prevent certain wallet addresses from transacting in their stablecoin (e.g., blacklisting) or to remove stablecoins from circulation on the secondary markets (i.e., freezing or burning).”), <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf>; Jeffery A. Collins, Cryptocurrencies and Financial Crimes: The Role of Decentralized Cryptocurrency in Facilitating Money Laundering and the Challenges Posed on Anti-Money Laundering Regulations, 34 U. Miami Bus. L. Rev. 71, 71–72 (2025) (“To address these vulnerabilities, the paper proposes three solutions: mandating privacy-preserving technologies like zero-knowledge proofs for mixing services, requiring decentralized identity solutions for cryptocurrency ATMs and DEXs, and enhancing public education on cryptocurrency risks and safe practices.”), <https://repository.law.miami.edu/umbl/vol34/iss1/5/>. For views that recognize at least some difficulties involved in enforcing AML/CFT regulations in fully decentralized ecosystems, see Francesco Paolo Patti, Towards a Global Anti-Money Laundering Law for Crypto-Assets, 56 Geo. J. of Int’l Law 697 (2025), [9](https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2025/12/GT-</p></div><div data-bbox=)

[GJIL250031.pdf](#); Jingyi Wang, Dancing with the Devil? Decentralized Finance (DeFi), Its Challenges, and Possible Regulatory Solutions, 26 UC Davis Bus. L. J. 2 (2026), <https://blj.ucdavis.edu/sites/g/files/dgvnsk15221/files/2026-05/Page%201%20-%20Dancing%20with%20the%20Devil.pdf>. Congress recognizes the practicability of requiring payment stablecoin issuers to have “the technological capability to comply” with a lawful order, which includes one that “requires a person to “seize, freeze, burn, or prevent the transfer of payment stablecoins issued by the person.” GENIUS Act, Pub. L. No. 119-27, sec. 8, 139 Stat. 419, 450 (July 18, 2025) (codified at 12 U.S.C. § 5907(a)(1); *id.* § 5901(16).

Gov’ts will find ways to respond to emerging blockchain risks. For example, Polymarket is a blockchain-based prediction market platform that allows users to speculate on the outcome of real-world events from popular culture, weather, sports, economics, and politics. It operates on the Polygon network and denominates transactions in the USDC stablecoin. *See* Karl Montevirgen, “Polymarket: American predication market platform,” *Britannica Money* (July 26, 2026), <https://www.britannica.com/money/Polymarket>. Concerned that Polymarket could expose users to significant gambling losses and that some wagers on the platform can be manipulated, France’s national gambling regulator recently instructed French internet service providers to block access to Polymarket’s website. *See* Sudip Kar-Gupta, “France blocks access to Polymarket website,” *Reuters* (July 17, 2026), <https://www.reuters.com/technology/french-internet-service-providers-told-block-access-polymarket-2026-07-17/>.

¹¹ **Non-controlling providers are often transmitting money.** *See* Letter from Nat’l Ass’n of Asst. U.S. Attorneys to Members of the Senate Committee on Banking, Housing, and Urban Affairs, at 1 (Jan. 14, 2026) (“The proposal to carve out certain ‘non-controlling’ developers or service providers from being treated as money transmitting businesses under federal or state law solely because they create or publish software, enable self-custody, or provide distributed ledger infrastructure raises significant concerns. While the proposal attempts to limit this carve-out to defined activities, the provision nonetheless creates a statutory carveout that defendants are likely to invoke to challenge unlicensed money transmitting charges. Many financial crime operations intentionally avoid traditional custody or unilateral control while still facilitating, routing, and monetizing transactions for users. By elevating formal control as a threshold requirement, this change to the criminal code risks shielding conduct that current law properly treats as money transmission.”), <https://www.politico.com/f/?id=0000019b-c7ef-d22e-a1db-dfff83de0000>.

¹² **Exempting mixers & tumblers is terrible policy.** *See, e.g.*, FATF, Targeted Report on Stablecoins and Unhosted Wallets (Peer-to-Peer Transactions), at 12 (Mar. 2026) (“In this example, DPRK actors laundered the stolen funds through mixers, cross-chain bridges, and over 125,000 Ethereum wallets, indicating quick, high-volume transactions likely intended to complicate tracing.”), <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf>.

¹³ **Front-Ends.** *See, e.g.*, airfocus by Lucid, “Front End (in a Website)” (visited June 24, 2026) (“When building a digital product, the question, ‘What is a front-end?’ goes beyond just design aesthetics. It’s about creating the entire user-facing experience, from layout and navigation to how users interact with features. . . . The front end of a website is everything the user either sees or interacts with when they visit the website. It is responsible for the total look and feel of an online experience.”), <https://airfocus.com/glossary/what-is-a-front-end/>; Paul Tierno, CRS Report R48883, An Overview of Decentralized Finance (DeFi), at 7 (updated Apr. 17, 2026) (“Interface layer. ‘Front end’ applications are interfaces through which users interact with the programs built on underlying layers.”), https://www.congress.gov/crs_external_products/R/PDF/R48883/R48883.6.pdf; U.S. Treasury, Illicit Finance Risk Assessment of Decentralized Finance, at 8 (Apr. 2023) (“The application tier – front-end user interfaces, application programming interfaces (APIs), and other code that allow participants to interact with the smart contracts and are primarily hosted off-chain.”), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>; U.S. Securities and Exchange Commission, Staff Statement Regarding Broker-Dealers Registration of Certain User Interfaces Utilized to Prepare Transactions in Crypto-Asset Securities (Apr. 13, 2026) (“For purposes of this statement, a ‘Covered User Interface’ is an interface provided by a website, browser extension, or other software application (*e.g.*, mobile application) that may be embedded in a wallet or separately available for download, designed to assist users engaging in user-initiated crypto asset securities transactions on blockchain protocols (or blockchain-based smart contracts) utilizing the user’s self-custodial wallet. Covered User Interfaces typically provide functionality with respect to any type of crypto asset transaction.”), <https://www.sec.gov/newsroom/speeches-statements/staff->

[statement-regarding-broker-dealer-registration-certain-user-interfaces-utilized-prepare-staff-statement-regarding-broker-dealer-registration-certain-user-interfaces-utilized.](#)

¹⁴ **RegTech.** *See, e.g.,* Capgemini, Reimagining KYC: From legacy friction to the pKYC triad, at 12 (2026) (“The pKYC [perpetual Know Your Customer] triad—data modernization, intelligent automation, and intelligent analytics—forms the operating core of the perpetual model. * * * Together, they create a durable regulator-ready framework that detects risk faster, reduces operational burden, strengthens defensibility, and improves CX [customer experience]”), <https://www.capgemini.com/wp-content/uploads/2026/02/FCC-WHITEPAPER-web-locked.pdf>; Transmit Security, Simplifying Compliance with AML & KYC, Technical White Paper, at 1 (2023) (“This white paper is designed to help enterprises understand how Transmit Security can help them overcome challenges with AML and KYC through secure digital onboarding and how to orchestrate, monitor and maintain frictionless journeys throughout the customer lifecycle with natively integrated identity security services.”), <https://content.transmitsecurity.com/hubfs/White-Papers/AML-KYC-whitepaper.pdf>.

As far back as 2020, some firms—RegTech firms—developed software for AML purposes and marketed it to financial institutions. *See, e.g.,* White Paper, The Future of KYC Compliance: How to embrace digital KYC to overcome the challenges of today and seize the opportunities of tomorrow (2020), <https://knowyourcustomer.com/wp-content/uploads/2020/06/Future-of-KYC-Compliance-White-Paper-2.pdf>; *id.* at 18–22 (stating that digital KYC will be characterized by agile planning, agile technology, agile technology set-up, and agile scope to set up and maintain the four pillars of the KYC process: document collection, data assessment, reporting & intelligence, and ongoing monitoring).

These firms provide services for secure customer onboarding, strong identity-verification technology, facial-matching technology, risk assessments, multi-layer identify verification, and digital audit trails. *See, e.g.,* Thales, Best Practices for Digital Customer Onboarding for Financial Institutions, White Paper (visited June 24, 2026), <https://cpl.thalesgroup.com/resources/access-management/digital-onboarding-best-practices-white-paper>; Transmit Security, Simplifying Compliance with AML & KYC, Technical White Paper, at 9–11 (2023) (discussing identity verification, customer identification, customer due diligence, and recordkeeping), <https://content.transmitsecurity.com/hubfs/White-Papers/AML-KYC-whitepaper.pdf>.

¹⁵ **Sanctions Law.** U.S. sanctions law has traditionally applied to all U.S. persons. *See* U.S. Dept. of Treasury, Office of Foreign Assets Control (OFAC), “11. Who must comply with OFAC sanctions?” (Aug. 21, 2024) (“All U.S. persons must comply with OFAC sanctions, including all U.S. citizens and permanent residents regardless of where they are located, all individuals and entities within the United States, and all U.S. incorporated entities and their foreign branches.”), <https://ofac.treasury.gov/faqs/11>; 31 CFR 591.312 (defining a U.S. person as “any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.”); Edward J. Collins-Chase, CRS R47829, Sanctions Primer: How the United States Uses Restrictive Mechanisms to Advance Foreign Policy or National Security Objectives (Nov. 6, 2023), https://www.congress.gov/crs_external_products/R/PDF/R47829/R47829.3.pdf.

¹⁶ **Smart Contracts.** *See* Paul Tierno, CRS Report R48883, An Overview of Decentralized Finance (DeFi), Overview (updated Apr. 17, 2026) (“Smart contracts are pieces of code that self-execute when certain requirements are met. They are essential to the variety of services offered, [including those offered by] mixers”), https://www.congress.gov/crs_external_products/R/PDF/R48883/R48883.6.pdf; *id.* at 5–6 (explaining how users interact with smart contracts, rather than with traditional financial institutions, to execute certain digital-asset transactions); U.S. Treasury, Illicit Finance Risk Assessment of Decentralized Finance, at 8 (Apr. 2023) (stating that people use front-ends to access smart contracts and execute digital-asset transactions); Niloufer Selvadurai, Mitigating the Legal Challenges Associated with Blockchain Smart Contracts: The Potential of Hybrid On-Chain/Off-Chain Contracts, 80 Wash. & Lee L. Rev. 1163 (2023), <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4830&context=wlulr>.

¹⁷ **Van Loon & IEEPA.** *See Van Loon v. U.S. Dept. of Treasury*, 122 F.4th 549, 563–566 (5th Cir. 2024) (interpreting 50 U.S.C. § 1702(a)(1)(B)); International Emergency Economic Powers Act (IEEPA), Pub. L. No. 95-223, 91 Stat. 1625 (1977) (codified at relevant part 50 U.S.C. § 1702(a)(1)(B) (authorizing the President to prohibit transactions “involving any property” meeting certain conditions); Steven A. Levy, Notice & Comment, *Van Loon v. Dept. of*

Treasury – A Decision with Important Implications for Bitcoin, Yale J. on Reg. (Dec. 2024), <https://www.yalejreg.com/nc/van-loon-v-department-of-the-treasury-a-decision-with-important-implications-for-bitcoin-by-steven-a-levy/>.

¹⁸ **Crypto-Kiosk Bill.** See S. 710, Crypto ATM Fraud Prevention Act of 2025, 119th Cong. (2025); *see also* HR 9268, Stop Crypto ATM Scams Act, 119th Cong. (2026) (proposing to amend the BSA to require the registration of digital asset kiosk operators and to require them to comply with AML and anti-fraud requirements).

¹⁹ See Senators Tim Scott, Chair, Senate Banking, & Senator John Boozman, Chair, Senate Agriculture, “Market Structure Legislation: Provisions Strengthening Law Enforcement” (July 22, 2026), <https://www.lummis.senate.gov/wp-content/uploads/One-Pager-Law-Enforcement-Provisions-1.pdf>.

²⁰ See Kuzi Charamba, Yan Yue Joyce Shum, & Douglas W. Arner, “Building Castles in the Sky? The Myth of Decentralized Finance and the Necessity of Legal Ordering, 25 Wash. U. Global Stud. L. Rev. 1, 27 (2025) (“The [IOSCO] report clarifies the misconception that DeFi products, services, and activities are materially different from those offered in traditional financial markets. In fact, they substantially mirror the operation of the traditional financial markets, with the only difference being the means with which such activities are carried out—the former uses DLT [distributed ledger technology] to varying degrees. Another misconception concerns the human elements involved in the decentralized financial system. Activities in DeFi are not carried out in a fully automated manner as what is commonly perceived by participants. Instead, there is significant human involvement in the delivery of DeFi products and services, as well as in the design, deployment, operation, and maintenance of the codes that implement a DeFi protocol, which demonstrates a close resemblance to the operation of the traditional markets.”), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5796883.

²¹ See, e.g., CLARITY Act, section 10109 (124:16–17; 125:12–126:6) (attempting to freeze the principles of, and the judicial precedent interpreting, the securities laws and regulations as they are in effect on the day before CLARITY’s enactment), section 10301 (166:7–14; 173:1–174:10) (attempting to freeze SEC’s and Treasury’s authority under the BSA as it was on the day before CLARITY’s enactment), section 10302 (176:17–18; 179:20–180:20) (attempting to freeze the laws governing economic sanctions, anti-money-laundering, and “any other illicit-finance laws” in effect as of the day before CLARITY’s enactment), section 10604 (309:10–12; 310:3–311:12) (attempting to exempt non-controlling developers and providers from “any registration requirement that is substantially similar to a requirement (as in effect on the day before the date of enactment of this Act) that applies to an entity described . . .”).

²² Kuzi Charamba, Yan Yue Joyce Shum, & Douglas W. Arner, “Building Castles in the Sky? The Myth of Decentralized Finance and the Necessity of Legal Ordering, 25 Wash. U. Global Stud. L. Rev. 1, 8–13 (2025) (categorizing the range of DeFi’s risks and misbehaviors to include governance risk; operational fragilities, including those inherent in smart contracts, oracles, and blockchain bridges; liquidity and maturity mismatches; leverage; and risk of complex interconnectedness between DeFi and the crypto-asset ecosystem), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5796883; *id.* at 9 (“The decentralized nature of the network gives rise to the risk of moral hazard due to the difficulty in establishing and enforcing accountability among those who launch DeFi projects through open protocols. This can expose investors to financial losses by fraud, rug-pulls, and other illegal actions by project developers and programmers.”); *id.* at 9–10 (“Smart contract risks as they relate to DeFi are typically in the form of insecurities. Smart contracts are simply automatically executing computer code: they are permanent, immutable, and non-reversible once triggered. They may or may not be contracts. They certainly are not smart, by definition in fact. Their inherent risks can manifest as a fraudulent transaction or a coding error, which, for instance, would allow hackers to manipulate token prices, steal funds, or drain investors’ crypto holdings . . .”).