NATIONAL SHERIFFS' ASSOCIATION

May 13, 2026

The Honorable Tim Scott
Chairman
Senate Committee on Banking,
Housing, and Urban Affairs
Washington, D.C. 20510

The Honorable Elizabeth Warren
Ranking Member
Senate Committee on Banking,
Housing, and Urban Affairs
Washington, D.C. 20510

Re: HR 3633, CLARITY Act, and Senate Banking's Proposed Amendment

Dear Chairman Scott and Ranking Member Warren:

Given that scammers defraud victims—often the elderly—of billions of dollars each year,[1] it's time to stand up for victims, potential victims, and law enforcement. The National Sheriffs' Association joins others in urging Congress to establish a regulatory framework for cryptocurrency and the digital-asset marketplace. Law enforcement needs the tools to follow transactions and trace funds or digital assets and—where probable cause links an account to fraud or other crime—freeze accounts and seize and recover funds for victims. Law enforcement also needs the tools to track and arrest scammers, and prosecutors need the tools to prosecute them.

In July 2025, Congress took a good first step in establishing a regulatory framework for payment stablecoins in the GENIUS Act.[2] The bill included a permitting system, granted rulemaking authority to regulate the various types of payment stablecoin issuers, established reserve requirements, and applied BSA obligations to all permitted payment stablecoin issuers.

In late May 2025, a representative introduced HR 3633, Digital Asset Market Clarity Act of 2025. The bill seemed like a good start at setting out a regulatory framework for traditional institutions like banks, other regulated financial institutions, and money services businesses to expand into the digital-asset marketplace.

In mid-January 2026, however, Senate Banking introduced an amendment in the nature of a substitute to HR 3633,[3] and, in the evening of May 11, it introduced a revised version.[4] Although it hasn't analyzed all 309 pages of the proposal, NSA has significant concerns. First, section 604 would exempt mixers, tumblers, and decentralized ledgers (DeFi) from regulations that govern money-transmitting businesses or persons engaged in money transmitting.[5] Section 604 would even try to exempt them from *future* registration requirements.[6] The purpose of mixers and tumblers is to "functionally obfuscate the source, destination, or amount in virtual asset transactions,"[7] which impairs law enforcement's ability to trace transactions and digital assets, and *recover victims' money*.[8] DeFi also enables illicit financial activity.[9] No good reason supports giving mixers, tumblers, and DeFi a blanket exemption.

While some software developers are not engaged in money transmitting or other activity that should subject them to BSA regulation,[10] plenty of others are. In its January 13, 2026 letter, for example, the National Association of Assistant United States Attorneys made this very point; that is, section 604's exemption for non-controlling developers or service providers "risks shielding conduct that current law properly treats as money transmission."[11]

Although the May 11 text includes new language that would clarify that 18 U.S.C. § 1960(b)(1)(C) would apply to a person who knowingly facilitates crime,[12] this edit will nonetheless leave participants in the digital-asset marketplace who *are engaged in money transmitting* largely unregulated. Moreover, exempting such participants from license and registration requirements will make it that much more difficult to identify the ones who knowingly facilitate crime.

NSA supports Senator Catherine Cortez Masto's proposed amendment to section 604. Not all software developers are engaged in money transmitting or other activity that should subject them to BSA/AML regulations. But others are. Senator Cortez Masto's proposal distinguishes between the two groups. Her proposal—which focuses on custody of users' digital assets, ability to transact, participation in an operation to facilitate digital-asset transfers between others, and compensation—would amend section 604 so that it would not provide a blanket exemption for all software developers, especially mixers, tumblers, and DeFi.

Far from addressing law enforcement's concerns,[13] moreover, the May 11 text would *expand* section 604's special treatment of mixers, tumblers, and DeFi. For example, section 301 would require the SEC, in consultation with Treasury, to adopt new rules for certain non-de-centralized finance trading protocols according to their activities. But new language would exempt mixers, tumblers, and other DeFi from such rules.[14] Section 302 would require Treasury to issue guidance for how DeFi front ends (user friendly graphical interfaces) must comply with AML/CFT and sanctions obligations. But new language would exempt mixers, tumblers, and other DeFi from the definition of a "financial institution" under applicable laws.[15] NSA supports Senator Catherine Cortez Masto's amendments to strike 159:22–23 from section 301 and to strike 166:8–11 from section 302.

Second, in the May 11 text, NSA sees no alternative framework to regulate mixers, tumblers, and DeFi. For example, section 205 of the amendment proposes to require digital-asset-kiosk operators to use distributed-ledger analytics to prevent a kiosk from sending a digital asset to a wallet known to be affiliated with fraudulent activity at the time of a kiosk transaction and to detect transaction patterns indicative of fraud or other illicit activities.[16] It would also require a kiosk operator to maintain restrictions that prevent more than one customer of the kiosk operator from using the same digital wallet address.[17] Thus, a regulation *can* require certain participants in the digital-asset marketplace to take steps to detect fraudulent activity and to freeze or stop a transaction to prevent the completion of a fraud.[18] It seems possible that a rule could even require software to contain protocols *internally* to detect and prevent fraud.[19] No good reason supports exempting mixers, tumblers, and DeFi from these efforts.

Third, although S. 710, Crypto-ATM Fraud Prevention Act of 2025, apparently served as the template for section 205 of the proposed amendment to HR 3633, the amendment would remove key provisions for potential scam victims and law enforcement. For example, the amendment proposes to alter a pre-transaction disclosure to customers,[20] reduce customer-refund provisions,[21] not to require digital-asset-kiosk operators to take reasonable steps to detect and prevent fraud,[22] and reduce protection for a new customer in a transaction.[23] It also wouldn't require a digital-asset-kiosk operator to submit its contact phone number and email address to FinCEN and all other relevant law enforcement.[24] These would also be poor policy choices.

In sum, Congress should regulate digital assets and the digital-asset marketplace. *All* participants in the digital-asset marketplace should be subject to regulations appropriate to their activity and risk. Even if Senate Banking's proposed amendment to HR 3633, CLARITY Act, is a start to establishing a regulatory framework for traditional financial institutions and other regulated entities to enter the marketplace, the proposed amendment has serious flaws in setting up a framework for non-traditional participants. Some will use evolving software, algorithms, and agentic AI to help transfer digital assets without tracing or accountability, launder money, finance terrorism, and evade sanctions. Section 604's proposal to exempt mixers, tumblers, and DeFi from registration, KYC, AML, and BSA regulations under the fiction that they all simply write code is bad policy. NSA supports Senator Catherine Cortez Masto's amendments to sections 301, 302, and 604.

As always, the nation's sheriffs appreciate your hard work in support of public safety and welfare.

Sincerely,

Sheriff Chris West
Canadian County, OK
President
National Sheriffs' Association

Justin Smith
Executive Director, CEO
National Sheriffs' Association

Cc: Senator Catherine Cortez Masto

Endnotes

[1] *See, e.g.*, Internet Crime Complaint Center, 2025 IC3 Annual Report, at 3 ("For the past quarter-century, IC3 has been the primary connection between the FBI and the public for information related to cyber-enabled criminal activity. Since our founding, reporting to IC3 has surged. We received a few thousand complaints per month in our early days. We now average almost 3,000 complaints per day. * * * In 2025, losses reported to IC3 continued to climb, surpassing the $20 billion mark."), https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf; Joanne Binette, AARP, "Fraud is Everywhere and It Affects All of Us" (Apr. 7, 2026) ("Fraud, resulting in stolen money or information, continues to be a widespread consumer issue, with many Americans experiencing financial loss, or adjusting behaviors to reduce risk. New AARP research finds that while most adults worry about fraud and are aware of scam tactics, many everyday activities continue to leave consumers exposed."), https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/2026-fraud-survey/; Luke Balcombe, "The Mental Health Impacts of Internet Scams," 22 Int'l J. Environ. Res. Public Health 938 (June 2025) (reporting that scam victims suffer profound shame and embarrassment, emotional distress such as anxiety and depression, and trauma), https://pmc.ncbi.nlm.nih.gov/articles/PMC12192844/.

[2] *See* GENIUS Act, Pub. L. No. 119-27, 139 Stat. 419 (July 18, 2025).

[3] *See* "Senate Banking Chair Releases Amended Version of 'Digital Asset Market Clarity Act,'" US Regulatory Intelligence (Jan. 15, 2026), https://www.findknowdo.com/news/01/15/2026/senate-banking-chair-releases-amended-version-digital-asset-market-clarity-act.

[4] https://www.banking.senate.gov/imo/media/doc/ehf26374.pdf

[5] *See* Amend. No. _ to HR 3633, sec. 604 (EHR26374 MSS) (May 11, 2026) (271:12–21) (defining a non-controlling developer or provider as "a developer or provider of a distributed ledger service that, in the regular course of operations, does not have the legal right or the unilateral and independent ability to control, initiate upon demand, or effectuate transactions involving digital assets to which users are entitled, without the approval, consent, or direction of any other third party."), https://www.banking.senate.gov/imo/media/doc/ehf26374.pdf; Amend. No. _ to HR 3633, sec. 604 (EHR26374 MSS) (May 11, 2026) (271:22–272:23) (exempting non-controlling developers and providers from treatment as a money-transmitting business under 31 U.S.C. § 5330 or as a person engaged in money transmitting under 18 U.S.C. § 1960).

[6] *See* Amend. No. _ to HR 3633, sec. 604 (EHR26374 MSS) (May 11, 2026) (272:8–14) (providing that a non-controlling developer or provider will not be "otherwise subject to 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" a money-transmitting business or a person engaged in money transmitting).

[7] Dept. of Treasury, Illicit Finance Risk Assessment of Decentralized Finance, at 10 (Apr. 6, 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[8] *See, e.g.*, 171 Cong. Rec. S1347–48 (daily ed. Feb. 25, 2025) (Statement of Sen. Richard Durbin) (telling the story of a Chicago man who lost $15,000, which disappeared in a crypto-ATM kiosk, as a result of a scammer impersonating a deputy sheriff and threatening the victim with arrest); Dept. of Treasury, 2026 National Money Laundering Risk Assessment, at 53 (Mar. 2026) ("Criminals commonly use obfuscation tools, services, and methods that introduce challenges for investigators attempting to trace illicit digital assets. These tools and services include mixers, anonymity-enhancing cryptocurrencies (AECs), and money laundering services through darknet markets. In addition to selling illicit drugs and other contraband, darknet markets often offer money laundering services, mixing digital assets used for purchases of goods and services from the market. In some instances, illicit actors may deposit funds and subsequently withdraw them from darknet markets without making a purchase as a laundering technique."), https://home.treasury.gov/system/files/246/2026-NMLRA.pdf.

[9] *See, e.g.*, Paul Tierno, Cong. R. Serv., R48883, An Overview of Decentralized Finance (DeFi), at 17–20 (Mar. 16, 2026) (discussing DeFI and illicit financial activity); U.S. Dept. of Treasury, Illicit Finance Risk Assessment of Decentralized Finance, at 1 (Apr. 2023) ("The assessment finds that illicit actors, including ransomware cybercriminals, thieves, scammers, and Democratic People's Republic of Korea (DPRK) cyber actors, are using DeFi

services in the process of transferring and laundering their illicit proceeds. To accomplish this, illicit actors are exploiting vulnerabilities in the U.S. and foreign AML/CFT regulatory, supervisory, and enforcement regimes as well as the technology underpinning DeFi services. In particular, this assessment finds that the most significant current illicit finance risk in this domain is from DeFi services that are not compliant with existing AML/CFT obligations:"), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[10] DOJ, Speech, "Acting Assistant Attorney General Matthew R. Galeotti Delivers Remarks at the American Innovation Project Summit in Jackson, Wyoming" (Aug. 21, 2025) ("Our view is that merely writing code, without ill-intent, is not a crime. Innovating new ways for the economy to store and transmit value and create wealth, without ill-intent, is not a crime. The Criminal Division will, however, continue to prosecute those who knowingly commit crimes — or who aid and abet the commission of crimes — including fraud, money laundering, and sanctions evasion. When bad actors exploit new technologies, it undermines public trust in those technologies and stifles innovation."), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-matthew-r-galeotti-delivers-remarks-american.

[11] 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 carve-out 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] *See* Amend. No. _ to HR 3633, sec. 604 (EHR26374 MSS) (May 11, 2026) (272:24–273:7), https://www.banking.senate.gov/imo/media/doc/ehf26374.pdf.

[13] *See, e.g.*, Letter from Nat'l Sheriffs' Ass'n to Hon. Tim Scott, Chair, Senate Banking, and Hon. Elizabeth Warrant, Ranking Member, Senate Banking, at 1 (Mar. 17, 2026) (pointing out that section 604 would create a broad exemption for certain non-controlling developers or providers, which could significantly limit the applicability of the AML/BSA statutes"), https://www.sheriffs.org/wp-content/uploads/2026/04/Letter-from-Sheriffs-HR-3633.pdf.

[14] *See* Amend. No. _ to HR 3633, sec. 301 (EHR26374 MSS) (May 11, 2026) (159:22–23) ("[None of SEC's or Treasury's new rules under section 301(b), (c)] may be construed to . . . (B) apply to non-controlling developers or providers, as defined in section 604(b)(3) . . . ."), https://www.banking.senate.gov/imo/media/doc/ehf26374.pdf.

[15] *See* Amend. No. _ to HR 3633, sec. 302 (EHR26374 MSS) (May 11, 2026) (166:8–11) ("Nothing in this section may be construed to . . . expand or contract the applicability of . . . (B) the definition of a 'financial institution' under applicable laws, which shall not apply to non-controlling developers or providers, as defined in section 604(b)(3) . . . ."), https://www.banking.senate.gov/imo/media/doc/ehf26374.pdf.

[16] S. 710, Crypto-ATM Fraud Prevention Act, would require a kiosk operator to use blockchain analytics to prevent sending virtual currency to a wallet known to be affiliated with fraudulent activity at the time of a kiosk transaction and to detect transaction patterns indicative of fraud or other illicit activities. *See* S. 710 (11:14–21). S. 710 would also authorize Director, FinCEN, to request evidence from any kiosk operator to confirm compliance with the analytics requirements. S. 710 (11:22–25). HR 3633, sec. 205, contains similar provisions. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (130:22–140:2; 146:11–19; 147:1–3).

[17] See Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (146:20–24).

[18] *See, e.g.*, Secretary of Treasury, Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets, at 22–27 (Mar. 2026) (discussing the possible uses of blockchain monitoring and analytics to trace and attribute illicit activity in digital assets and ending with six recommendations including an intention for Treasury to work with industry to understand best practices and technical requirements for implementing blockchain analytics tools in AML/CFT compliance),

https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.

[19] *See, e.g.*, Beth Stackpole, MIT Mgt. Sloan School, "Agentic AI, explained) (Feb. 18, 2025) ("'The agent could raise a red flag or even be programmed to stop a conveyor belt if there was a problem,' [Professor Sinan] Aral said. 'It is not just the digital world — agents can actually take actions that change things happening in the physical world.'"), https://mitsloan.mit.edu/ideas-made-to-matter/agentic-ai-explained.

[20] For example, S. 710 would require a kiosk operator to provide a consumer a statement that the customer should contact the . . . kiosk operator's customer service helpline or State or local law enforcement if they suspect fraudulent activity." S. 710 (6:14–17; 8:1–4). In contrast, HR 3633 sec. 205, would require a kiosk operator to provide a consumer a statement that the consumer should contact law enforcement alone if they suspect fraudulent activity or a scam along with a relevant agency's contact information. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (143:7–11).

[21] In a post-transaction receipt, for example, S. 710 would require a notice that a customer may be entitled to a refund as a matter of law and a copy of the kiosk operator's refund policy. S. 710 (8:11–14; 9:1–10). In contrast, in a similar receipt, HR 363, sec. 205, omits all reference of a possible refund and only advises the customer to contact law enforcement if he or she suspects fraud. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (143:21–24, 144:11–151). In another example, S. 710 requires a kiosk operator to issue a refund to new customers for the full amount of each kiosk transaction, including the dollar value of virtual currency exchanged and all transaction fees, made during the period for which the customer was a new customer and was fraudulently induced to engage in the kiosk transaction. S. 710 (12:25–13:1–12; 13:23–14:15). S. 710 also has a provision under which an existing customer may receive a refund of transaction fees in some circumstances. S. 710 (13:13–22). In contrast, HR 3633, sec. 205, would provide only for a refund of transaction fees in certain circumstances involving fraud. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (148:8–24). Also, S. 710 would permit a customer to recover up to 3 times the amount of a refund owed or $10,000, whichever is greater, from a kiosk operator who denies a refund in violation of the provision. S. 710 (14:16–22).

[22] S. 710 specifically would require a kiosk operator to "take reasonable steps to detect and prevent fraud . . . ," S. 710 (9:25–10:1–3), while HR 3633, sec. 205, would contain no such language. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (144:23–145:20).

[23] Before permitting a new customer to enter a kiosk transaction valued at $500 or more, S. 710 would require a kiosk operator to obtain a *verbal* confirmation from the new customer that the customer (1) wishes to proceed with the transaction, (2) understands transaction's nature, and (3) is not being fraudulently induced to engage in the transaction. S. 710 (12:1–14; 12:20–24 (requiring a verbal confirmation via a live phone or video call to an employee of the kiosk operator)). HR 3633, sec. 205, wouldn't require a verbal confirmation (just a confirmation), and it would omit the understanding confirmation. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (147:4–12). Second, S. 710 would require a kiosk operator to make a reasonable effort to determine whether the customer is being fraudulently induced to engage in a kiosk transaction, S. 710 (12:15–19), while HR 3633, sec. 205, wouldn't, Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (147:4–17). HR3633, sec. 205, would, however, require a kiosk operator to delay executing a transaction on a new customer's behalf that sends digital assets to a specific wallet address until 72 hours have elapsed since the new customer initiated the transaction. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (147:13–17). It's difficult to assess the value of this because HR 3633, sec. 205, doesn't confer a right to cancel the transaction on the new customer.

[24] S. 710, for example, would require kiosk operators to provide a dedicated and frequently monitored phone number and email address for relevant law-enforcement and government agencies to facilitate communication with the kiosk operator in the event of reported or suspected fraudulent activity. S. 710 (15:18–24). Moreover, S. 710 would require kiosk operators to submit their contact information to FinCEN and all other relevant law-enforcement and government agencies. S. 710 (16:1–6). In contrast, HR 3633, sec. 205, would only require kiosk operators to post a phone number, email address, "or other contact method" on a sticker on the ATM. Amend. No. _ to HR 3633, sec. 205 (EHR26374 MSS) (May 11, 2026) (149:11–18). It's difficult to think of a less effective measure.