BLOCKCHAIN ASSOCIATION

August 3, 2026

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

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

Re: The National Sheriffs' Association's July 31, 2026 Letter Concerning the Digital Asset Market Clarity Act

Dear Majority Leader Thune and Minority Leader Schumer:

The National Sheriffs' Association ("NSA") is right that Congress must take illicit finance seriously. That is what the Digital Asset Market Clarity Act ("the Clarity Act" or "the Act") does.[1] The NSA's July 31 letter and attachment (together, the "NSA Letter"), however, fundamentally misconstrues the legislation it asks the Senate to reject. The NSA Letter repeatedly describes a bill that Congress did not write. It claims the Clarity Act exempts decentralized finance, mixers, bridges, software developers, and user interfaces from anti-money laundering and sanctions laws writ large. It also claims the Act strips regulators of authority and leaves law enforcement with fewer tools.[2] The Clarity Act does none of those things.

Further, NSA's position does not reflect a law enforcement consensus. The Fraternal Order of Police, the National Organization of Black Law Enforcement Executives, the Major Cities Chiefs Association, and the Federal Law Enforcement Officers Association support the legislation.[3] Major County Sheriffs of America withdrew its opposition and adopted a neutral position.[4] A coalition of 160 former national security, intelligence, and law enforcement officials has also urged the Senate to advance the Act.[5] That record forecloses any suggestion that NSA's interpretation reflects the consensus of the law enforcement community.

---

[1] Section references to the Act refer to the July 22, 2026 Senate discussion draft of H.R. 3633.
[2] Letter from Sheriff Troy Wellman, President, National Sheriffs' Association, and Justin Smith, Executive Director and CEO, National Sheriffs' Association, to Senators John Thune and Charles E. Schumer (July 31, 2026), attaching National Sheriffs' Association, Regulating the digital asset Marketplace and CLARITY (July 29, 2026) (the "NSA Letter attachment"), at 2–5.
[3] *See* Letter from Patrick Yoes, National President, Fraternal Order of Police, to Timothy E. Scott, Chairman, and Elizabeth A. Warren, Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs (July 24, 2026) (supporting the most recent version of H.R. 3633 after reviewing the revised developer-protection provision); Letter from Renée Hall, National President, National Organization of Black Law Enforcement Executives, to John Thune, Senate Majority Leader, and Charles E. Schumer, Senate Democratic Leader (July 1, 2026) (formally endorsing the Act); Jasper Goodman, *Sheriffs Group Says Crypto Bill Has "Significant Law Enforcement and Public Safety Risks,"* POLITICO PRO (July 31, 2026) (reporting that the Major Cities Chiefs Association backed the legislation); Federal Law Enforcement Officers Association, *FLEOA Supports H.R. 3633 While Recommending Targeted Refinements to Preserve and Strengthen Federal Law Enforcement Protections* (July 10, 2026).
[4] *See* Major County Sheriffs of America Drop Opposition to CLARITY Act, BeInCrypto (July 4, 2026) (reporting and quoting MCSA's July 3 letter stating that it was "now neutral on H.R. 3633").
[5] Letter from 160 Former National Security, Intelligence, and Law Enforcement Officials to John Thune, Senate Majority Leader, and Charles E. Schumer, Senate Democratic Leader (June 3, 2026) (urging the Senate to advance the Act and stating that it would improve law enforcement visibility and strengthen investigative tools).

NSA reaches its conclusion by starting from a policy premise found nowhere in federal law or generally recognized standards: that every person who earns revenue in connection with a transaction in digital assets – regardless of how far removed they are from the transaction or its counterparties – should be regulated as a financial institution. The Bank Secrecy Act ("BSA") does not use that test; neither does longstanding guidance from the Financial Crimes Enforcement Network ("FinCEN") or the international standards adopted by the Financial Action Task Force ("FATF"), which NSA invokes. NSA's approach would impose bank-like duties on people who do not hold customer assets, transmit value, know the identity of the user, or control the transaction.[6]

The Clarity Act draws the line in a more sensible place that is supported by existing law. The Act regulates intermediaries based on what they do and the control they exercise over funds and transactions. Firms that hold customer assets, execute transactions, or operate certain controlled financial services face substantial regulatory obligations under the Act. At the same time, the Act makes clear that developing neutral software or providing infrastructure does not, by itself, turn someone into a regulated actor. Think of the common sense distinction between a neutral third-party cloud or other communication service provider and a financial institution itself. That distinction does not protect criminals or unregistered businesses. To the contrary, Clarity imposes rigorous obligations on actual intermediaries and gives law enforcement the tools to work with them to provide greater defenses against financial crime than exist today in the absence of Clarity's framework.

Blockchain Association and its members have prepared this response to address the primary arguments made in the NSA Letter and dispel its most misleading claims.

I. NSA's proposed rule to regulate "everyone who receives revenue" is neither existing law nor reflective of the FATF standard.

NSA states that Congress should regulate "everyone who receives revenue" from the digital asset marketplace.[7] The NSA Letter cites no federal statute, regulation, or standard that has ever adopted such a broad approach.

For purposes of regulating an actor under the BSA, FinCEN looks at what the person actually does. Money transmission generally requires accepting currency, funds, or other value from one person and transmitting it to another person or location.[8] FinCEN has made clear that creating and distributing software, without more, does not qualify as the acceptance and transmission of value.[9] The receipt of revenue also does not solely establish that the person is providing a covered financial service that triggers registration and reporting requirements under the BSA. A person who

[6] NSA Letter attachment at 1 (proposing regulation of "everyone who receives revenue" from the digital asset marketplace).
[7] Id.
[8] *See* 31 C.F.R. § 1010.100(ff)(5).
[9] Financial Crimes Enforcement Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019).

uses software to provide a covered financial service may be regulated. The receipt of revenue does not establish that the person is providing such a service.[10]

FATF takes the same general approach. Its definition of a virtual asset service provider ("VASP"), a term generally describing a financial intermediary, applies when a person, as a business, performs exchange, transfer, custody, administration, or specified issuer-related services "for or on behalf of" someone else. FATF guidance does not treat a person acting solely as a developer, unhosted-wallet software provider, validator, or network infrastructure provider as a VASP unless that person also performs a covered function or retains sufficient control over funds or transactions.[11]

NSA is therefore proposing an unprecedented and extreme regulatory regime. Its revenue test would reach actors both within the blockchain ecosystem and across the broader internet economy – including validators, node operators, data providers, cloud service providers, and internet service providers – regardless of whether they have customers, take custody of assets, or exercise discretion over transactions. Congress should not impose the obligations of a financial institution on parties that perform fundamentally different functions and therefore lack the practical ability to satisfy them.

II. The Act imposes substantial BSA and sanctions obligations on the intermediaries capable of carrying them out.

NSA claims that Section 10201 would regulate "practically no one." The text of that section says otherwise. It brings digital commodity brokers, digital commodity dealers, and digital commodity exchanges that are registered, or required to register under the Act, fully within the BSA framework. Those firms must maintain robust anti-money laundering ("AML") and countering the financing of terrorism ("CFT") programs, assess their risks, establish internal controls, appoint compliance officers, train employees, and undergo independent testing. They must also retain transaction records, monitor and report suspicious activity, identify customers, conduct customer due diligence, and comply with Office of Foreign Assets Control ("OFAC") sanctions.

These are the principal customer-facing intermediaries in the new federal framework. Other provisions establish CFTC registration and regulation for digital commodity exchanges, custodians, brokers, dealers, associated persons, pool operators, and trading advisers. Firms operating under the provisional notice regime during implementation remain subject to supervision and examination. Provisional registrants also must comply with requirements governing disclosures, records, financial responsibility, cybersecurity, conflicts of interest, and customer assets. Describing this framework as an exemption requires disregarding both the Act's registration provisions and the BSA amendment that expressly applies to firms registered or required to register under them.

---

[10] *Cf.* SEC Division of Trading and Markets, Staff Statement Regarding Broker-Dealer Registration of Certain User Interfaces Utilized to Prepare Transactions in Crypto Asset Securities (Apr. 13, 2026) (fees are not dispositive of regulatory treatment as a broker-dealer).

[11] Financial Action Task Force, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers ¶¶ 59–60, 76, 82–83 (Oct. 2021).

The Act also addresses the use of decentralized protocols by regulated intermediaries. Before conducting trading activity through such a protocol, an intermediary must assess the risks of money laundering, sanctions evasion, fraud, manipulation, operational failures, and cybersecurity incidents. The intermediary must maintain appropriate monitoring capabilities and establish procedures for executing, rejecting, or suspending transactions when risks are identified. Regulators may examine compliance, and FinCEN and OFAC retain their investigative and enforcement authority. To be clear, these provisions put more watchful eyes from responsible actors on financial crime, not fewer.

III. The statutory text forecloses NSA's claim that the Act creates a blanket exemption for decentralized finance.

NSA describes Section 10301 as "a big exemption."[12] In fact, it is an affirmative directive to regulate. Section 10301 directs the SEC, in consultation with Treasury, to write rules for persons who control protocols that are decentralized in name only and perform intermediary functions. A controlled financial business cannot escape regulation simply by calling itself decentralized. That is the purpose of this section.

Section 10301 identifies circumstances when a protocol may not be genuinely decentralized. These include circumstances in which a person or group of persons can control or materially alter its functions, operations, or rules; its operation depends on discretionary rather than pre-established and transparent code; or a person can restrict or censor its use. When those conditions are present, the SEC must issue rules applying the relevant requirements associated with the functions the controlling person actually performs, including acting as a broker or dealer, facilitating trading, executing transactions, clearing transactions, and providing custody.

Treasury must also adopt tailored BSA rules for controlling persons whose securities registration makes them financial institutions under existing law. Until that rulemaking is complete, Section 10301 creates no presumption that a person or activity is either covered or exempt. It also expressly preserves the SEC's and Treasury's investigative and enforcement authority. Section 10301, therefore, does the opposite of removing controlled systems from regulation. It gives the agencies an affirmative mandate to regulate the people behind them according to the financial functions they perform.

To take the NSA's own example – where "platforms won't be *fully* autonomous" – Section 10301 is specifically designed to *cover* these platforms under anti-money laundering and countering the financing of terrorism requirements of the Bank Secrecy Act, not to provide them an exemption.

NSA repeats the same error when discussing mixers, tumblers, and cross-chain bridges. Nothing in the Act exempts them from any law or regulation. Their treatment depends on who is involved, what functions they perform, the control they retain, and the conduct of those who control the systems.

---

[12] NSA Letter attachment at 2.

Section 10309 separately directs Treasury, DOJ, and State and local law enforcement to examine mixer and tumbler typologies, illicit use, and potential legislative or regulatory responses. NSA may believe Congress should take a different approach, but a mandated study is not a grant of immunity. Further, NSA's assertion that cross-chain bridges are necessarily "transaction obfuscating services" is a categorical (and inaccurate) statement that provides no basis for disregarding the Act's functional tests.

The Act's other software provisions are similarly limited. Sections 10601 and 20209 provide that specified development and infrastructure activities, standing alone, do not trigger intermediary regulation under the securities laws or the Commodity Exchange Act. Both provisions preserve authority over fraud, manipulation, and false reporting. The result is that anyone who uses software or infrastructure to defraud users or manipulate markets remains subject to those laws.

IV. Section 10604 clarifies money transmitter status for non-controlling developers without immunizing criminal conduct.

One of NSA's most consequential errors concerns the Blockchain Regulatory Certainty Act in Section 10604. That provision applies only to a "non-controlling developer or provider." To qualify as such, a person must lack both the legal right and the unilateral, independent ability to control, initiate on demand, or carry out transactions involving users' digital assets.

The provision establishes a consistent standard for determining when non-controlling developers are treated as money transmitters under regulatory and criminal law. Specifically, a qualifying non-controlling developer is not treated as a money transmitting business merely because that person creates or maintains software, provides self custody tools, or supplies infrastructure support. Section 10604 expressly preserves money transmitter and financial institution treatment based on conduct outside that limited scope. It also preserves the application of 18 U.S.C. § 1960(b)(1)(C) to a person who acts with the specific intent to transfer, on behalf of another person, funds the person knows are criminal proceeds or are intended to promote unlawful activity.

Nothing in Section 10604 amends the federal money laundering statutes, wire fraud statute, conspiracy law, aiding-and-abetting law, sanctions law, terrorism financing statutes, narcotics laws, theft or fraud offenses, or forfeiture authority. A developer or service provider who launders proceeds, conspires with criminals, violates sanctions, defrauds users, or operates an unlicensed money transmitting business remains subject to prosecution.

V. NSA's other objections overlook language that answers them directly.

Front end interfaces. Section 10302 addresses U.S.-owned or operated web-hosted applications through which users submit transaction instructions. It directs Treasury to issue guidance addressing sanctions and AML/CFT obligations, blockchain analytics screening, sanctioned wallets and jurisdictions, ransomware, illicit finance indicators, and controls for blocking or rejecting prohibited transactions. Section 10302 does not in any way diminish Treasury's existing power; it expressly preserves the government's ability to administer and enforce sanctions and illicit finance laws.

Sanctions. NSA points to *Van Loon v. Department of the Treasury*[13] as a means to raise a separate issue under the International Emergency Economic Powers Act ("IEEPA"): whether the immutable smart contracts at issue in that case qualified as sanctionable "property." The Clarity Act does not repeal IEEPA, narrow sanctions against identifiable persons, or impede the prosecution of sanctions violations.

Section 10303 of the Act gives Treasury an additional tool modeled on Section 311 of the USA PATRIOT Act. When Treasury finds a primary money laundering concern involving a foreign jurisdiction, foreign financial institution, or class of transactions, it may prohibit or condition specified digital asset transmittals by domestic financial institutions and agencies. Regulated intermediaries must comply with OFAC requirements, and sanctions enforcement remains available against U.S.-operated front ends. Congress may consider a tailored IEEPA amendment separately. Its absence from this bill does not create an exemption.

Digital Asset Kiosks. NSA also greatly understates the protections governing digital asset kiosks. Section 10205 requires fraud warnings, customer acknowledgments, receipts, anti-fraud policies, a designated compliance officer, blockchain analytics, wallet controls, and confirmation that specified new customers are not acting under fraudulent inducement. It also includes a 72-hour holding period, cancellation rights, refunds of transaction amounts and fees, transaction limits, customer service access, and law enforcement coordination.

Temporary holds. Section 10305 encourages good faith temporary holds when a firm reasonably suspects unlawful activity or receives a qualified written request from law enforcement. The firm must comply with documentation, notice, and court order requirements. The liability protection removes a significant reason firms might otherwise hesitate to cooperate.

NSA is also incorrect in stating that traditional financial institutions face the same litigation risk "with no liability shield."[14] Existing federal law protects financial institutions and their personnel for qualifying disclosures of suspected violations.[15] It separately protects certain notifications to the government[16] and provides a safe harbor for qualifying law enforcement "keep open" requests.[17] Section 10305 applies a similar principle to digital asset transactions that may otherwise settle irreversibly.

Regulatory authority. The provisions NSA describes as a regulatory "freeze" are largely savings clauses.[18] They preserve existing authority while preventing the implementation of the Act from being treated as an implied expansion or contraction of agency power.

---

[13] 122 F.4th 549 (5th Cir. 2024).
[14] NSA Letter attachment at 5.
[15] *See* 31 U.S.C. § 5318(g)(3)(A).
[16] *See* 12 U.S.C. § 3403(c).
[17] *See* 12 U.S.C. § 1960(b); 31 U.S.C. § 5333(a).
[18] NSA Letter attachment at 5.

NSA also urges Congress to "clearly commit the tasks of studying, reporting on, and regulating the digital asset marketplace and all participants to the appropriate agencies."[19] Importantly, the Act requires new rulemakings and recurring reports. It directs the government to examine mixers, foreign intermediaries, foreign adversary activity, cybersecurity, and financial stability risks.[20] It also establishes mechanisms for international coordination and requires federal financial regulators to report to Congress on the implementation of the Act and any legislative changes that may be needed.[21] Congress has not merely authorized regulators to respond as risks change. It has required them to.

VI. The Act gives local law enforcement substantial new resources.

The NSA Letter gives little weight to Title IX, which provides significant new resources to law enforcement. Section 10902 authorizes $600 million per year for fiscal years 2027 through 2031, totaling $3 billion. State and local agencies may use those funds for investigations and prosecutions involving digital assets, sanctions evasion, fraud, terrorism financing, and other illicit finance. The funding also supports training and the use of blockchain analytics tools and other investigative technologies. Section 10903 establishes a joint Treasury and DOJ training and technical assistance program for Federal, State, local, Tribal, and territorial officers, investigators, prosecutors, and analysts.

Section 10904 establishes a Digital Asset Cyber Innovation Center focused on disrupting criminal activity, sharing threats in real time, responding to emergencies, and recovering assets. The Act creates a Treasury-led task force to prevent scams and help recover victims' funds. It also supports information sharing with State and local law enforcement and establishes an interagency working group focused on terrorism, narcotics trafficking, and illicit finance.

FinCEN would receive an additional $30 million annually for five years to strengthen its technology, policy, examination, information sharing, and enforcement capabilities. These provisions respond directly to the practical challenges facing sheriffs and local investigators.

* * *

The Clarity Act places obligations on customer-facing intermediaries, people who control nominally decentralized protocols, and regulated firms that route activity through decentralized systems. It preserves the criminal and sanctions laws that apply to everyone. It also gives law enforcement new authority, funding, analytics, training, and recovery tools.

---

[19] *Id.*

[20] *See* Clarity Act Sections 10309 (study on digital asset mixers and tumblers), 10310 (GAO study on intermediaries in foreign jurisdictions), 10311 (studies on foreign adversary activities), 10312 (study on cybersecurity standards), and 10313 (studies on financial stability risks).

[21] *See* Clarity Act Sections 10502 (international cooperation, including coordination with foreign regulators, information sharing arrangements, cooperative enforcement, and cross-border regulatory sandboxes), 10507 (international coordination to combat digital asset illicit finance), 10508 (annual reports on foreign jurisdictions' digital asset activity, compliance with U.S. standards, and remediation efforts), and Section 10504 (reports from federal financial regulators that must include any legislative recommendations).

The Senate should therefore reject NSA's request to delete Section 10604 and to impose BSA status on every revenue recipient, interface, developer, or infrastructure provider. It should evaluate the legislation Congress actually wrote, preserve the distinction between financial intermediaries and neutral technology, and support law enforcement by enacting Clarity's measures aimed at identifiable actors who control assets, operate financial services, or knowingly assist criminal activity.

Respectfully,

Summer Mersinger
CEO, Blockchain Association