October 17, 2025
VIA ELECTRONIC TRANSMISSION

Julie Lascar
Director, Office of Strategic Policy, Terrorist Financing and Financial Crimes
Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Re: Department of the Treasury Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets

Dear Director Lascar:

Blockchain Association respectfully submits this letter in response to the Department of the Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets. 90 Fed. Reg. 40148 (Aug. 18, 2025). The Department issued the Request as directed under Section 9(a) of the GENIUS Act, Public Law 119–27, 139 Stat. 419.

Blockchain Association is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for the digital asset economy. The Association works to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can create a more secure, competitive, and consumer-friendly digital marketplace. The Association represents over 130 member companies reflecting the wide range of participants in the blockchain industry, including software developers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem.

The Association shares the Department's interest in preventing the use of digital assets for illegal purposes. Many of the Association's members are active and trusted partners of law enforcement and regulators across the globe, and regularly take action to assist law enforcement in identifying and preventing money laundering and countering the financing of terrorism ("CFT") even when doing so goes beyond their legal obligations.

The Association also welcomes clear, pro-innovation rules from the Department to govern the Bank Secrecy Act's ("BSA") application to the digital asset economy. The Department should act now by adopting reasonable regulations through notice-and-comment rulemaking to resolve the uncertainty that plagued the last Administration's approach to these issues and to ensure a stable regulatory framework going forward. Those regulations should be guided by four principles. *First*, the regulations should place no greater burdens on digital asset companies than those applicable to firms in traditional finance. *Second*, the regulations should account for the heightened privacy concerns implicated by blockchain transactions. *Third*, to encourage continued innovation in anti-money-laundering ("AML") techniques, the regulations should be principles-based, tech-neutral, and functional, rather than prescribing any particular technological solutions or tools for discharging AML obligations. *Fourth*, the Department should act quickly to issue legislative rules on these and other issues through the notice-and-comment process. By adopting clear, stable,

and reasonable regulations, as swiftly as possible, the Department can support this Administration's goal of making the United States a leader in the digital asset industry.

I. Illicit-finance risks are, if anything, lower in the digital asset ecosystem

This section responds to Question 1 of the Request for Comment: "In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem?" 90 Fed. Reg. at 40150. The Association shares the government's goals of preventing money laundering and countering the financing of terrorism. Association members (as well as other digital asset companies) have long worked closely with federal law enforcement to fight illicit finance. Coinbase, for example, has trained thousands of federal law-enforcement officers in crypto-specific investigative techniques, and it works with the U.S. Marshals Service to maintain digital assets seized in law enforcement actions.[1] Coinbase and Kraken have assisted U.S. law enforcement in identifying victims of "pig butchering" schemes and seizing approximately $225 million in fraud proceeds in 2025.[2] Circle holds an inaugural three-year seat on the board of directors for the Illicit Virtual Asset Notification, a public-private partnership designed to identify and prevent illicit digital asset activity.[3] Chainalysis is a contracting party with the U.S. government, and has offered employees to testify as experts in criminal trials brought by the Department of Justice.[4] And these are just a few illustrative examples of the broader industry's longstanding commitment to ensuring that bad actors do not exploit blockchain technology for criminal purposes.

As with traditional finance, digital assets can be used for illicit purposes, but those risks are not greater than the illicit-finance risks in traditional finance. To the contrary, the public, permanent, and transparent nature of blockchain technology makes it easier to detect, trace, and prevent illicit transactions. Accordingly, regulations issued by the Department should not require more of

---

[1] Testimony of Grant Rabenn, Director, Financial Crimes Legal at Coinbase Before the U.S. House Committee on Financial Services Subcommittee on Digital Assets, Financial Technology, and Inclusion, at 7 (Feb. 15, 2024), https://tinyurl.com/yj5dxfkd ("[W]e have offered crypto investigations training, free of charge, to thousands of law enforcement officers around the world. . . . Our philosophy is that the better law enforcement understands crypto and the ways in which public blockchains can be analyzed to detect and investigate criminal activity, the more effectively they can safeguard our customers and the ecosystem as a whole."); Brett Tejpal & Greg Tusar, *U.S. Marshals Service chooses Coinbase to safeguard, trade its large cap digital assets portfolio*, Coinbase (July 1, 2024), https://tinyurl.com/mt7d42f5.

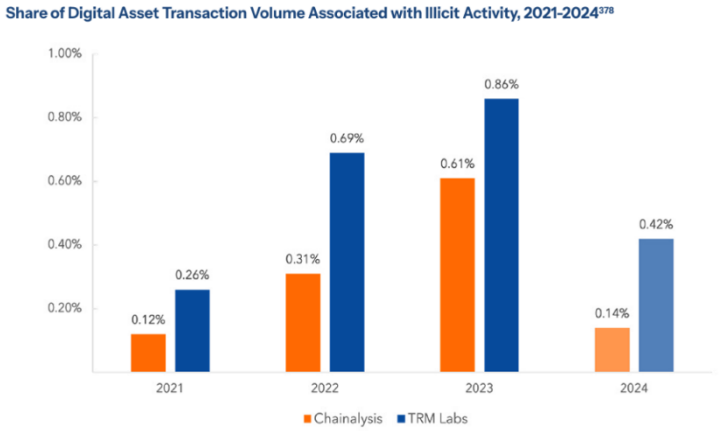
[2] *Kraken assists U.S. Secret Service in record-breaking crypto fraud seizure*, Kraken (July 3, 2025), https://tinyurl.com/36k9x64v; *Consumer Protection Tuesday: How Coinbase Helped the Secret Service Seize $225M in Stolen Crypto*, Coinbase (June 24, 2025), https://tinyurl.com/hrx35nxm.

[3] *Circle Appointed to Board Position on U.S. Government-led Partnership to Combat Illicit Finance*, Circle (Oct. 2, 2024), https://tinyurl.com/ye93jcdp.

[4] *CONTRACT to CHAINALYSIS INC.*, USASpending.gov, https://tinyurl.com/yrunx8ph (last accessed October 16, 2025); Press Release, *United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars*, Justice.gov (Nov. 5, 2020), https://tinyurl.com/y6nrp6ph ("The forfeiture action is the result of an investigation by IRS – Criminal Investigation Cyber Crimes Unit with assistance from Chainalysis and Excygent."); *United States v. Sterlingov*, 719 F. Supp. 3d 65 (D.D.C. 2024) (describing expert testimony by Elizabeth Bisbee of Chainalysis).

participants in the digital asset industry than the Department requires of traditional financial institutions.

The Report by the President's Working Group on Digital Asset Markets, *Strengthening American Leadership in Digital Leadership in Digital Financial Technology* ("Working Group Report"), notes that "[d]espite increasing over the last decade, the prevalence of money laundering and terrorist financing via digital assets remains well below that of the same activities utilizing fiat currency, bank and traditional money services fund transfers, and other methods that do not involve digital assets."[5] The Working Group Report also quotes Association member Chainalysis's illustration that less than 1% of digital asset transaction volume between 2021 and 2024 was associated with illicit activity:[6]



By contrast, the United Nations estimated in 2020 that around $1.6 trillion per year, or 2.7% of global GDP, is laundered in fiat currency.[7]

Although the Working Group Report notes illicit-finance risks related to digital assets, such as jurisdictional arbitrage, service providers who fail to comply with their AML/CFT and sanctions obligations, and anonymity-enhancing technologies, none of those concerns is unique to digital assets.[8] In 2024, the Department highlighted that "[t]he centrality of the United States in cross-border payments and banking means the U.S. financial system is inextricably linked with the broader international financial system," which allows "[s]ophisticated illicit actors" to "exploit" "jurisdictional arbitrage" by forming or registering companies and opening accounts in "jurisdictions with weaker AML/CFT legal frameworks and supervisory systems and less developed mechanisms for international cooperation."[9] The Department has repeatedly brought enforcement actions against traditional financial institutions that have failed to comply with their AML

[5] Working Group Report at 101.

[6] *Id.* at 102.

[7] U.N. Dep't of Econ. & Soc. Affs., *Tax abuse, money laundering and corruption plague global finance* (Sept. 24, 2020), https://tinyurl.com/38s8ztyz.

[8] Working Group Report at 102.

[9] Department of the Treasury, *2024 National Strategy for Combating Terrorist and Other Illicit Financing*, at 18 (May 2024), https://tinyurl.com/59ce73ds.

obligations.[10] And illicit actors can use traditional markets to evade scrutiny of their true identities: even ordinary assets such as used cars can be purchased and sold in money laundering schemes.[11] FinCEN has continuously warned of the dangers of trade-based money laundering schemes, including by Chinese money laundering networks to launder illicit cartel funds.[12] These illicit-finance risks are, if anything, reduced in the crypto context due to the public and transparent nature of blockchain transactions.

II. AML rules should account for the heightened privacy concerns in the digital asset context

Illicit-finance risks are only one side of the AML equation. AML laws, like all laws requiring private parties to turn over information to the government, must balance the government's law-enforcement interests against the privacy interests of individuals. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001) ("[T]he reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.") (quotation marks omitted); *Carpenter v. United States*, 585 U.S. 296, 303 (2018) (The "basic purpose of [the Fourth] Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."); *cf. Cal. Bankers Ass'n v. Shultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring) (cautioning against overreach under the BSA because "the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate").

Transactions in digital assets raise heightened privacy concerns compared to traditional financial transactions. Public blockchains are ledgers containing a permanent, public record of every transaction that has ever occurred on the blockchain—information that is available to any person in the world with an internet connection. Although many blockchain transactions are pseudonymous, meaning they do not have personally identifying information associated with them on the blockchain, once a person's name is connected to even a single blockchain transaction, it is often possible to reconstruct that person's entire transaction history, particularly when using advanced blockchain analytics.[13] And the information that can be gleaned about an individual can go beyond ordinary financial data. Blockchains today have social-network applications, facilitate the ownership and transfer of art via non-fungible tokens, and are used to make charitable donations. All of that information (and more) can be linked to an individual once the person's identity is linked to a public blockchain address.

Due to the vast quantities of information available about individuals on a blockchain, AML rules can create serious privacy risks and constitutional concerns, particularly to the extent that they require service providers to record and maintain information linking a person's identity to wallet addresses. Mandating that digital asset companies collect such information could allow hostile governments and other bad actors—which have historically attempted to hack financial institutions, digital asset

---

[10] *See, e.g.*, *In the Matter of TD Bank, N.A. and TD Bank USA, N.A.*, 2024-02 (Oct. 10, 2024).

[11] FinCEN, *Used Car Trade-Based Money Laundering Scheme*, https://tinyurl.com/69sm2w58; FinCEN, *SARs Aid Investigators in Case Where an Auto Dealer Laundered Drug Proceeds* (Oct. 2011), https://tinyurl.com/mrx5ptj9.

[12] FinCEN, *FinCEN Issues Advisory and Financial Trend Analysis on Chinese Money Laundering Networks* (Aug. 28, 2025), https://tinyurl.com/msjvbyky.

[13] Virginie Liebermann & Michel Molitor, *Blockchain vs Data protection*, International Network of Privacy Law Professionals (July 30, 2024), https://tinyurl.com/bdh4kwzx.

companies, and U.S. government agencies—to obtain an individual's entire financial history.[14] If repressive or hostile regimes or other bad actors gain access to detailed, de-anonymized transaction data, including sensitive transactions such as donations to religious or political organizations, that could put individuals at risk of harm.

Requiring digital asset companies to collect vast amounts of private, user-identifying information and make it available to the government also raises serious Fourth Amendment concerns. The Fourth Amendment generally bars the government (without a warrant) from requiring "third parties" to disclose "records in which [an individual] has a reasonable expectation of privacy." *Carpenter*, 585 U.S. at 317. And many individuals have a reasonable expectation of privacy in their transaction history on a blockchain, which can reveal the quintessential "privacies of life." *See id.* at 311. Moreover, digital asset companies have an independent Fourth Amendment right not to be compelled to collect and report "voluminous" private information about their users to the government. *See, e.g.*, *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 474-75, 486 (S.D.N.Y. 2019) (Fourth Amendment violation where law required rental company to produce "voluminous" data about its customers). Any AML rules the Department issues under the Bank Secrecy Act or any other statute must account for these constitutional concerns.

III. The Department's regulations should encourage continued innovation in crypto AML techniques

This section responds to Questions 2 through 6 of the Request for Comment regarding "innovative or novel methods, techniques, or strategies . . . financial institutions us[e] to detect illicit activity and mitigate illicit finance risks involving digital assets." 90 Fed. Reg. at 40151. The digital asset industry thrives on innovation. Bitcoin is less than 20 years old, and in that time has expanded from a concept in a pseudonymous white paper to an asset currently with a market capitalization of more than $2.1 trillion.[15] Digital asset technology is constantly progressing. Any rules or guidance regarding the industry's use of AML tools should account for the rapidly changing technological environment in which the industry operates and take care not to stunt innovation by imposing prescriptive practices that inhibit flexibility in the future.

As just a few examples, several Association members already employ innovative tools to identify customers, report suspicious activities, and freeze or block certain transactions without relying on users' personally identifiable information.

- A Zero Knowledge Proof is a method for one party to cryptographically prove to another that a statement is true (*e.g.*, "I have the right to transfer this asset") without revealing any information beyond the validity of the statement itself. The computation process for verifying the statement is committed to polynomials such that inputs to the computation may remain hidden.[16] In the context of privacy tools, a Zero Knowledge Proof allows a user to prove certain information to a digital asset company—including that the user is not on a list of sanctioned individuals or affiliated with sanctioned organizations—without revealing

[14] *See* Sean Lyngaas, *Exclusive: US Government Agencies Hit in Global Cyberattack*, CNN (June 15, 2023, 10:03 PM), https://tinyurl.com/yc75b8kr; *Timeline of Cyber Incidents Involving Financial Institutions*, Carnegie Endowment for International Peace (last updated in 2022), https://tinyurl.com/3zpwn554.

[15] CoinMarketCap, *Cryptocurrency Prices, Charts And Market Capitalizations*, https://tinyurl.com/3nnexf4s (last accessed October 16, 2025).

[16] *See* Vitalik Buterin, *An approximate introduction to how zk-SNARKs are possible* (Jan. 26, 2021), https://vitalik.eth.limo/general/2021/01/26/snarks.html.

any personally identifying information.[17] The Zero Knowledge Proof therefore serves the government's interest in preventing illicit transactions on blockchains without encroaching on users' privacy interests. And this is not just a theoretical concept: Association member the ZCash Foundation, for example, has implemented Zero Knowledge Proofs to ensure user balances and transaction history are accurate.[18] And Aleo Network Foundation, another Association member, has built a layer-1 blockchain secured by Zero Knowledge Proofs where transactions are private by default but the architecture supports selective disclosure and the ability to confirm user credentials without users having to reveal extraneous personal details.[19]

- In 2023, Coinbase introduced an innovative system that helps predict the potential riskiness associated with a particular blockchain address. One component of the system uses aggregate transaction behaviors of an address and graph-based features to capture structural and transactional information. The system then uses that information, in combination with a predictive machine-learning model, to generate a risk score for the address.[20]

- Chainalysis's Know Your Transaction product flags transactions based on indicators of risky behavior, such as the identity of the entity behind a counterparty. Chainalysis matches blockchain addresses that users send to or receive from with real-world entities that control them, which allows users to determine whether the counterparty to the transaction is a legitimate exchange or an illicit marketplace.

- Predicate builds novel policy infrastructure that enables developers, financial institutions, and digital asset organizations to implement AML/CFT policies directly into their smart contract platforms. Once integrated by an application at the smart contract level, every transaction submitted by a user is validated by an on-chain cryptographic attestation issued by Predicate's infrastructure. Attestations are issued with sub-second latency and only transactions that include an attestation from Predicate can be successfully processed by the smart contract. This architecture ensures that compliance cannot be bypassed by malicious users, who must always interact with the smart contract with a cryptographic attestation.[21]

- The Plume (Ethereum layer 2) blockchain has pioneered on-chain AML screening at the sequencer and smart contract level. Through an integration with Forta, transactions on the Plume network are screened against an illicit wallet database directly at the sequencer node, preventing sanctioned addresses from interacting with the Plume blockchain. In addition to sanctions screening, Plume performs real-time detection of smart contract exploits, rug pulls, phishing, fake tokens, as well as private key compromises (in certain

---

[17] *What Is Zero-Knowledge Proof in KYC Verification*, Zyphe.com (Sept. 5, 2025), https://tinyurl.com/5b7t64xr.

[18] *What are zero-knowledge proofs?*, ZCash, https://tinyurl.com/3ct4bdy9.

[19] *What is Aleo, the privacy-first blockchain?*, Aleo.org (Oct. 19, 2023), https://tinyurl.com/mr3dmnc5.

[20] *See* Ayush Agarwal, *Detecting Fraudulent Transactions: Coinbase Scalable Blockchain Address Risk Scoring System*, Coinbase (Dec. 6, 2023), https://tinyurl.com/3acx84un.

[21] *See* Lesley Chavkin et al., *A Risk Management Framework for Institutional Liquidity on Uniswap V4*, Predicate.io, https://tinyurl.com/ycmtmwza.

scenarios). Plume also works with Predicate in connection with the Plume-developed Nest DeFi protocol. With Predicate, Nest smart contracts block transactions originating from high-risk addresses, leveraging risk-score data from TRM Labs, Inc. to identify high-risk addresses beyond sanctions.

- zPass is a decentralized credential system that allows a user to submit a "proof" of verified data, such as passport information.[22] The verified credential proof is stored on the Aleo blockchain, but can be accessed online by anyone to whom the user gives permission, giving users control over their personal digital data. This approach eliminates the need to share the actual underlying document and keeps personal identity information safe from hacks, thefts, forgeries, and cybersecurity risk associated with online services storing user data themselves. Users can create these proofs without requiring modification from, or coordination with, identity-issuing authorities. zPass has already been used successfully in other non-financial contexts, such as for age verification to protect children using online services.[23] Fully decentralized applications can also be programmed to accept zPass credentials configured for a range of parameters. For example, blockchain software developers could choose to create a decentralized exchange that allows users to withdraw assets only if their zPass credential shows that they are not on the OFAC Specially Designated Nationals list and other sanctions lists.

Given this rapid innovation, it is critical that the Department's rules allow market participants to continue to develop novel AML solutions without being straitjacketed by prescriptive requirements that they use specific tools or practices. That approach would foster further innovation in the industry as it seeks to comply with AML requirements.

This approach is also consistent with recent guidance FinCEN and banking regulators have issued, allowing more flexibility to financial institutions. For example, in June, FinCEN, the FDIC, OCC, and NCUA granted an exemption that allows certain financial institutions to use alternative means of collection of Taxpayer ID Number from third parties.[24] Director Gacki explained that the exemption "reduce[s] burden by providing banks with greater flexibility in determining how to fulfill their existing regulatory obligations without presenting a heightened risk of money laundering, terrorist financing, or other illicit finance activity."[25]

IV. The Department should issue clear rules through notice-and-comment rulemaking

The Request for Comment notes that the Department can proceed through "guidance or notice and comment rulemaking." 90 Fed. Reg. at 40149. To the greatest extent feasible, the Department should adopt regulations through the notice-and-comment process.

---

[22] John Reynolds, *Introducing zPass: Aleo's pioneering step toward privacy-preserving digital identity*, Aleo.org (Oct. 23, 2023), https://tinyurl.com/bdmr4223.

[23] Rene Reinsberg & Jane Khodarkovsky, *How zero-knowledge tools can help us verify age and protect privacy online,* The Hill (July 23, 2025), https://tinyurl.com/yhrk6f42.

[24] FinCEN, *FinCEN Permits Banks to Use Alternative Collection Method for Obtaining TIN Information* (June 27, 2025), https://tinyurl.com/49tjh4d4.

[25] *See Statement by FinCEN Director Andrea M. Gacki before the House Committee on Financial Services, Subcommittee on National Security, Illicit Finance, and International Financial Institutions*, FinCEN (Sept. 9, 2025), https://tinyurl.com/56kxe44u.

A. *The Department should adopt legislative rules after notice and comment*

The AML requirements applicable to digital assets have been uncertain in the United States for years, in part due to the last Administration's approach of making major policy decisions through enforcement actions rather than clear and generally applicable rules. Indeed, the only sources of guidance for the BSA's application to digital assets have been FinCEN interpretive guidance statements, administrative rulings, and enforcement actions.[26] None of these has "the force and effect of law." *Perez v. Mortg. Bankers' Ass'n*, 575 U.S. 92, 103 (2015). Indeed, on at least one occasion the Department of Justice argued that FinCEN's guidance interpreting the BSA could be disregarded *entirely*, which further undermined any reliance by digital asset companies on FinCEN's informal pronouncements.[27]

Specific regulations tailored to the industry and adopted through notice and comment will, by contrast, provide clarity and stability and will foster innovation. That will allow the industry to flourish, consistent with the Administration's goal to "make America the undisputed leader in digital assets, bringing massive investment and innovation to our country."[28] Unlike informal guidance and policies adopted through regulation-by-enforcement, notice-and-comment regulations can be repealed or replaced only through another round of notice-and-comment rulemaking, promoting stability in the law by preventing future administrations from rewriting the rules without advance notice to the public and an opportunity for public participation in the decision. *Perez*, 575 U.S. 92 at 101.

In the current uncertain and often changing regulatory environment, digital asset companies have hesitated to spend resources in the United States and investors have hesitated to invest. And time is of the essence: other countries have made dramatic inroads through clear legislation and regulation, and digital asset companies are paying heed.[29]

B. *The Department's regulations should reject obsolete prior guidance and adopt innovation-enhancing rules*

The Department should also reject the missteps of prior Administrations' approach to digital assets and adopt rules that will prevent illicit finance while enhancing innovation and safeguarding privacy.

As one example, the Department should withdraw the prior Administration's proposal to designate convertible virtual currency ("CVC") mixing as a primary money laundering concern under Section

---

[26] *See, e.g.*, *In the Matter of Binance Holdings Limited, et. al. d/b/a Binance and Binance.com* (Nov. 21, 2023) (FinCEN enforcement action for failure to comply with BSA as unregistered money transmitting business); *In the Matter of HDR Global Trading Limited*, et al. (Aug. 10, 2021) (FinCEN enforcement action for failing to comply with BSA as an unregistered futures commission merchant). The Department of Justice has also brought criminal charges for violations of the BSA against digital asset market participants. *E.g. United States v. Binance Holdings Ltd.*, 2:23-cr-00178 (W.D. Wash.) (Nov. 21, 2023); *United States v. Hayes*, 1:20-cr-00500 (S.D.N.Y.) (Oct. 1, 2020).

[27] *United States v. Storm*, 1:23-cr-00430 (S.D.N.Y.), Dkt. No. 53 (Apr. 26, 2024) (Department of Justice opposition to motion to dismiss), at 33 ("Fourth, even if it did support the defendant's argument, the FinCEN Guidance is not a regulation or rule and has no authoritative effect.").

[28] *Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law*, The White House (July 18, 2025), https://tinyurl.com/chutjkkm.

[29] For example, the European Union adopted the Markets in Crypto-Assets Regulation, which institutes uniform EU market rules for digital assets. The United Arab Emirates and Singapore have each also established clear and comprehensive regulations for digital assets.

311 of the PATRIOT Act.[30] This proposal represented the first time that FinCEN tried to use Section 311 to designate an entire class of transactions as of primary money laundering concern. FinCEN's findings did not come close to connecting the entire class of transactions with unlawful activity. Instead, FinCEN merely concluded that "CVC mixing transactions *can* play a central role in facilitating the laundering of CVC derived from a variety of illicit activity." (Emphasis added). FinCEN's statements in the proposal even recognized that many users conduct transactions involving CVC mixing for wholly lawful and legitimate conduct, such as protecting their privacy. If adopted, the proposed rule would stigmatize broad swathes of legitimate digital asset activity, impose significant costs on the digital asset industry, and drive illicit digital asset transactions abroad where they would be subject to reduced or no regulatory oversight and would be less accessible to U.S. law enforcement. The Department should target illicit use and facilitators while preserving lawful privacy-enhancing technologies—paired with advanced on-chain analytics and enforcement at regulated access points.

The Department should also clarify, ideally through notice-and-comment rulemaking, what its 2019 Guidance correctly recognized in the first place: that only entities that exercise "control" over assets can be subject to the BSA.[31] In two criminal cases brought during the last Administration, the Department of Justice misinterpreted the 2019 Guidance and incorrectly charged company executives with operating unlicensed money services businesses pursuant to 18 U.S.C. § 1960, despite the fact that the defendants did not control users' assets. *United States v. Storm*, 1:23-cr-00430 (S.D.N.Y.) (Aug. 23, 2023); *United States v. Rodriguez*, 1:24-cr-00082 (S.D.N.Y.) (Apr. 24, 2024).

In addition, the Department's regulations should not impose AML obligations on blockchain infrastructure providers because they do not control user assets. Blockchain infrastructure providers may include: hardware, software, and communications providers; miners, validators, delegators, and node operators; and providers of application programming interfaces ("APIs"), remote procedure calls, block explorers, and other data. Because infrastructure providers supply the passive infrastructure layer that facilitates the functioning of the blockchain network, they do not custody customer funds or assets. For example, miners and validators perform the important technical function of reviewing, verifying, and recording information. Similarly, other infrastructure providers do not interact with customers, hold assets, or otherwise engage in money services. They simply provide the technology (*e.g.*, hardware, software, communications, or data) layer that enables the networks to function and, if applicable, for other actors to conduct their activities. Any regulations the Department issues should explicitly protect developers and non-custodial infrastructure providers from inappropriate collection mandates of personally identifying information, reaffirming a functional, technology-neutral scope limited to custodial control of customer assets.

To promote innovation while ensuring strong compliance, the Department should pair principles-based rules with targeted safe harbors for properly governed APIs and artificial intelligence under the BSA, clarifying governance, human oversight, interoperability, testing, and recordkeeping expectations. The Department can support API adoption by establishing BSA safe harbors when firms use APIs to satisfy AML/CFT obligations. Firms should meet certain conditions to be eligible for a safe harbor (*e.g.*, governance or ongoing testing). Additional public-private collaboration and

[30] 88 Fed. Reg. 72701 (Oct. 23, 2023).

[31] FinCEN, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019).

regulatory sandboxes would also help the Department understand the appropriate scope of any safe harbors.

In addition, to limit exposure of personally identifiable information and avoid honeypot vulnerabilities, the Department should update customer-identification-program ("CIP")/know-your-customer rules to accept decentralized identity (DiD) credentials and Zero Knowledge Proofs as approved alternatives to document-based checks, allowing verification of status without disclosing underlying personal attributes. The Department can also update the CIP reliance framework so that institutions can rely on identity checks performed by a broader set of regulated parties, including money services businesses, enabling portable identities with one-time verification and repeated reuse, and redirecting compliance resources toward higher-risk cases.

Finally, though outside the scope of this comment letter, the Association also supports the Blockchain Regulatory Certainty Act currently being considered by Congress. If enacted, the Association believes that the Department should act quickly to issue rules implementing the law around money transmission for digital asset developers and service providers that do not custody consumer funds.

IV. Conclusion

The Association supports the Administration's fresh approach to the digital asset industry. President Trump has "promise[d] to position America as the global leader in cryptocurrency" and "emphasiz[ed] the need to embrace digital assets to drive economic growth and technological leadership."[32] Director Gacki has similarly recognized the urgent need to "modernize requirements under the BSA" and "reduce burden by providing [regulated entities] with greater flexibility in determining how to fulfill their existing regulatory obligations without presenting a heightened risk of illicit financial activity."[33] The Department's approach to innovative methods of combatting illicit activity in the digital asset industry should reflect this new and welcome approach to regulation in the digital asset industry.

Respectfully submitted,

/s/ Laura Sanders
Laura Sanders
Policy Counsel
Blockchain Association

cc: Stephanie Brooker
Nick Harper

---

[32] *Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law*, *supra* note 28.

[33] *See Statement by FinCEN Director Andrea M. Gacki*, *supra* note 25. Chairman Warren Davidson of the House Financial Services Subcommittee on National Security, Illicit Finance, and International Financial Institutions recently commented that "[o]ver decades, the Bank Secrecy Act has morphed into a bloated surveillance machine . . . FinCEN's own data shows . . . how this flood of paperwork buries real leads in bureaucracy instead of stopping bad actors." Press Releases, *Davidson: Over Decades, The Bank Secrecy Act Has Morphed Into A Bloated Surveillance Machine*, U.S. House Comm. on Fin. Servs. (Sept. 9, 2025), https://tinyurl.com/2evzvude.

Matt Gregory
Sam Raymond
Joy Wang
Gibson, Dunn & Crutcher