Comment of Coin Center on Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets

October 17, 2025
TREAS-DO-2025-0070-0001

To whom it may concern:

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

We thank the Department of the Treasury for the opportunity to comment on the *Innovative Methods to Detect Illicit Activity Involving Digital Assets*, issued pursuant to Section 9 of the *Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act.* The Treasury's interest in advancing both innovation and compliance is commendable. There are, indeed, many new technologies and techniques in development that could improve personal privacy while also enhancing crime-fighting and deterrence. The second half of this comment will highlight those technologies and propose areas of the stablecoin AML regime that could benefit. However, any new effort should begin with a clear understanding of the shortcomings of traditional AML practices at financial institutions, their failure to meet even modest cost and benefit analysis, the hazards they pose to individual freedom and dignity, and the particular danger they pose when mixed naively with open blockchain networks where transaction data is inherently public. The first half of this comment will outline these concerns and highlight constitutional and policy limits to data collection that must be adhered to as Treasury considers how to apply AML requirements to the stablecoin landscape.

I. Problems inherent in traditional AML Practices

Financial institutions today are burdened by identity verification frameworks that are simultaneously costly, privacy-invasive, and ineffective at deterring illicit finance. Despite vast surveillance systems built on the foundation of the Bank Secrecy Act (BSA), global authorities

estimate that less than 1% of criminal proceeds are ultimately recovered. Meanwhile, individuals are forced to repeatedly surrender their sensitive personal information to centralized databases at tremendous personal risk. Indeed, the very same personal information, when compromised in breaches, can be used to further evade such controls.

1. The Scale of the Problem: AML Is Vast, Costly, and Ineffective

For more than fifty years, the United States has relied on the Bank Secrecy Act (BSA) and its implementing regulations to deputize private financial institutions into surveillance intermediaries. Yet the record of success is vanishingly small. The United Nations Office on Drugs and Crime estimates that less than 0.2 percent of criminal proceeds are ultimately intercepted or recovered through AML enforcement.[1] Independent reviews by economists Ronald Pol and Michael Levi find that interception rates across comparable jurisdictions hover near 0.1 percent—a "near-zero impact on crime" despite enormous investment.[2]

Meanwhile, compliance costs have exploded. LexisNexis estimated U.S. financial institutions spend roughly $26 billion annually on AML and sanctions compliance, with global costs approaching $300 billion.[3] The resulting paperwork does little to prevent crime but imposes immense friction on lawful users, delays legitimate payments, and systematically excludes vulnerable populations from financial access.[4] Proponents of far-reaching AML and KYC controls may reply that low interception figures are beside the point: real success lies in deterrence—criminal transfers never attempted because an identity check stands in the way. That is a reasonable objection to our critique, but the available evidence suggests current methods may be deterring the wrong population.

The World Bank has warned that the "inappropriate implementation" of AML/CFT standards, particularly in emerging markets, "plays a role in excluding millions of low-income people from formal financial services."[5] More recent FATF stock-takes concede that their own standards have contributed to de-risking and financial exclusion, especially where institutions face high onboarding costs.[6] Ordinary customers with limited time and resources abandon or postpone account opening; sophisticated criminals, by contrast, adapt.

---

[1] United Nations Office on Drugs & Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes (2011).
[2] Ronald F. Pol, Anti-Money Laundering: The World's Least Effective Policy Experiment?, 3 Pol'y Design & Practice 191 (2020); Michael Levi & Peter Reuter, Money Laundering, 34 Crime & Just. 289 (2006).
[3] LexisNexis Risk Solutions, True Cost of Financial Crime Compliance: U.S. and Canada Edition (2020).
[4] World Bank, AML/CFT: Strengthening Financial Inclusion and Integrity (Focus Note No. 56, Apr. 2008).
[5] *Id.*
[6] Financial Action Task Force, High-Level Synopsis of the Stock-take of Unintended Consequences of the FATF Standards 4 (2021).
https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Unintended-Consequences.pdf

This evidence is summarized in Coin Center's report *Tear Down This Walled Garden: American Values and Digital Identity,* which documents how a half-century of surveillance-based identity verification has produced "enormous costs and privacy burdens for negligible benefit in stopping crime."[7]

In short, the current AML paradigm represents a failed experiment: a surveillance apparatus that is both ineffective and enormously expensive. Treasury's GENIUS-mandated inquiry should begin by recognizing that "more surveillance" is not synonymous with "more security."

2.. The Scale of the Harm: Ordinary People Bear the Burden

The same system that fails to stop sophisticated criminals routinely harms ordinary citizens. Traditional AML/KYC compliance demands the perpetual collection, duplication, and storage of intimate personal data—names, addresses, Social Security numbers, photos, and often biometrics. Each database becomes another honeypot for breach or abuse. The Federal Trade Commission reported over 1.1 million identity-theft complaints in 2022 alone, many stemming from data leaked by the very institutions charged with "protecting" consumers.[8]

When such information is abused by the state, the consequences are more severe. Coin Center's research documents how financial surveillance has been used worldwide to target political and religious minorities: in China's Xinjiang region, transaction data helped identify Uyghurs for detention; in Canada, authorities directed banks to freeze accounts of peaceful protestors without court orders.[9] Such examples are not distant hypotheticals—they demonstrate what can happen when a system built for AML becomes an infrastructure of control.

The United States has thus far avoided the most egregious abuses, but not by virtue of statutory restraint. As *Tear Down This Walled Garden* notes, "Law enforcement increasingly works hand-in-glove with financial institutions, obtaining virtually unchecked access to private financial data and testing out new methods of financial surveillance of American citizens."[10]

---

[7] Peter Van Valkenburgh & Ian Miers, Tear Down This Walled Garden: American Values and Digital Identity 5 (Coin Center 2025).
[8] Fed. Trade Comm'n, Consumer Sentinel Network Data Book 2022 (Feb. 2023).
[9] Geoffrey Cain, The Perfect Police State 135–38 (PublicAffairs 2021); Amanda Coletta, Trudeau Defends Using Emergency Powers Against Trucker Protests, Wash. Post (Nov. 25, 2022).
[10] U.S. House of Representatives, Financial Surveillance In The United States: How The Federal Government Weaponized The Bank Secrecy Act To Spy On Americans. Interim Staff Report of the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government. December 6, 2024, available at https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2024-12/2024-12-05-Financial-Surveillance-in-the-United-States.pdf

This practice rests on the brittle foundation of *United States v. Miller*, which denied Fourth Amendment protection to bank records in 1976.[11]

Beyond the measurable risks of data breaches and institutional abuse, financial surveillance exerts a quieter but equally corrosive effect on individual freedom. When people know that every transaction may be recorded, analyzed, or flagged, they begin to self-censor and avoid lawful but potentially stigmatized activity such as donating to controversial causes, supporting marginalized communities, or engaging in political dissent. The knowledge of constant observation breeds conformity and discourages experimentation, association, and expression. In this way, surveillance does not merely endanger privacy; it erodes the practical meaning of liberty itself by shaping citizens' choices before the state ever intervenes.

Altogether, a surveillance-based compliance regime inevitably corrodes privacy and freedom, while doing little to enhance safety. With the advent of stablecoins and the need to determine regulatory obligations for trusted issuers, we are now faced with two paths: do we carry over 1-1 costly and damaging AML policies from traditional finance or do we seek less invasive alternatives. As the remainder of this comment argues we must seek alternatives because the unique nature of stablecoins makes implementation of traditional AML methods even more corrosive of human rights and because technologies available and pioneered in the cryptocurrency ecosystem can out-perform existing practices while mitigating harms to personal privacy and freedom.

II. Naive Stablecoin AML Implementation Would Create a Perfect Panopticon

The GENIUS Act reasonably extends AML obligations to permitted payment-stablecoin issuers. Coin Center has long argued that persons who occupy positions of trust within cryptocurrency networks should be subject to the same regulatory treatment as those in equivalent positions within traditional finance—*same risk, same regulation*. Accordingly, an entity that issues and redeems a stablecoin should not be treated differently than an entity that issues and backs comparable real-world instruments. That principle, however, cuts both ways. When particular features of a stablecoin issuer's business create distinct or heightened privacy risks—especially risks to individuals who are not its customers—and when the application of traditional AML/KYC standards would exacerbate those risks to innocent third parties, *same risk, same regulation* requires a corresponding adjustment of regulatory obligations to mitigate those new harms.

[11] United States v. Miller, 425 U.S. 435 (1976).

Naive implementation of AML obligations—simply grafting existing BSA practices onto open blockchains—is far more invasive than the traditional regime. When real-world identity data collected by issuers is linkable to complete and detailed on-chain transaction history, every purchase, donation, or remittance becomes permanently traceable. Unlike the fragmented banking sector, where data are dispersed across thousands of institutions, a blockchain ledger is singular, global, and immutable. Once cross-referenced with off-chain identifiers, it yields an "intimate map of personal habits and associations"—a complete financial dossier available not only to regulators but also to hackers, foreign adversaries, and data brokers.[12]

This risk is not speculative. Sophisticated analytics firms already de-anonymize public blockchains comprehensively and with high accuracy.[13] A regulatory model that requires stablecoin issuers to collect, store, and retain identifying information while the corresponding transaction data remains public on-chain would deliver the very outcome civil libertarians fear from central bank digital currencies (CBDCs): a total financial panopticon. The issuer and the government can effectively see anything with little or no judicial oversight and, when this data is (inevitably) hacked or leaked, it can and will provide criminals and hostile foreign governments a complete dossier of the habits of innocent Americans.

Two technological developments can mitigate these risks. First, issuers can issue stablecoins on privacy-preserving blockchains where there is no public record of transaction data to be mixed with regulator-demanded KYC information from issuers and other regulated parties. Second, issuers can utilize new digital identity technologies, described below, to engage in data-minimized alternative AML compliance regimes.

III. Privacy-Preserving Blockchains, Stablecoins, and View Keys

Recent advances in privacy-preserving blockchain infrastructure now make it technically feasible to issue and manage stablecoins without sacrificing transactional privacy or regulatory oversight. These systems employ zero-knowledge proofs (ZKPs) and related cryptographic techniques to hide the details of individual transactions—amounts, counterparties, and balances—while still enabling verifiers to confirm that the system is solvent, compliant, and free of double-spending. Unlike earlier "mixer" models that merely obfuscated flows on public chains, modern privacy layers integrate proof systems that can mathematically guarantee correctness without revealing personal information. Networks such as Zcash, Aleo, Anoma,

[12] Peter Van Valkenburgh & Ian Miers, Tear Down This Walled Garden: American Values and Digital Identity (Coin Center 2025) .
[13] Kelvin Lubbertsen, Michel van Eeten & Rolf van Wegberg, Ghost Clusters: Evaluating Attribution of Illicit Services through Cryptocurrency Tracing, in Proceedings of the 34th USENIX Security Symposium (USENIX Ass'n 2025), https://www.usenix.org/conference/usenixsecurity25/presentation/lubbertsen.

Aztec, and Miden exemplify this new generation of privacy-preserving ledgers, combining programmable smart contracts with shielded transactions verifiable by third parties. Even on public chains, like Ethereum, new smart-contract based applications like Privacy Pools can allow stablecoin users to achieve reasonable personal privacy. Unlike previous tools like Tornado Cash, Privacy Pools even afford users the ability to avoid joining anonymity sets that include known bad actors like hackers.[14]

These new privacy-preserving networks allow peer-to-peer transactions to occur without creating a public record of the participants or the details of their payments. Stablecoin issuers operating on these blockchains can still perform all required AML and sanctions screening at the points of issuance and redemption—the processes they already own and control—even as users freely transact among themselves. The result is a system that preserves institutional oversight where it is most effective while protecting ordinary users from the unnecessary exposure of their financial lives. Instead of publishing an immutable, globally visible record of every cup of coffee, donation, or political contribution, these architectures enable lawful private exchange backed by cryptographic assurance rather than mass surveillance. While this may seem radical to some, it is nothing new: for centuries, banks have issued and redeemed convertible notes to their customers, ensuring that they understood their counterparties and the attendant risks, yet those notes circulated through the economy with no surveillance or monitoring at all. As Jerry Brito has noted,

> Cash is essential to an open society. It is an escape valve that lets us protect our privacy, dignity, and autonomy. It is therefore imperative that we preserve our ability to use it. Yet that is not enough. As we move to an increasingly online world in which physical cash is not practical for many transactions, we must also develop and foster electronic cash.[15]

Therefore, Treasury should not only permit but actively encourage stablecoin issuance on privacy-preserving blockchains and support users on public blockchains who wish to move their stablecoins through privacy tools like Privacy Pools. Doing so would align with the GENIUS Act's mandate to foster innovation and strengthen the integrity of U.S. digital financial technology. Stablecoins deployed on transparent public chains that link identities to transactions risk creating an irreversible surveillance infrastructure; those built on privacy-preserving substrates, by contrast, can meet compliance goals through cryptographic assurance rather than bulk data collection. In this sense, privacy-preserving blockchains and

[14] Ameen Soleimani et al., Privacy Pools: Exploring Practical Compliance Solutions for Privacy-Enhancing Technologies (2023), https://docs.privacypools.com/.
[15] Jerry Brito, "The Case for Electronic Cash 1.0," February 2019. https://www.coincenter.org/the-case-for-electronic-cash/#the-moral-case-for-electronic-cash

smart contracts are not a regulatory loophole—they are a regulatory upgrade: a way to achieve the same policy outcomes while dramatically reducing risks to personal privacy, cybersecurity, and civil liberties. Treasury should make clear that use of such systems is consistent with the Bank Secrecy Act and, through guidance, help demonstrate that the future of compliance is privacy by design, not surveillance by default.

In the context of privacy-preserving blockchains, some have proposed "view-key" systems whereby stablecoin issuers or government agencies could decrypt on-chain transactions on demand. This approach misunderstands both cryptography and civil liberties. Coin Center worries that some may offer view-keys as the trade-off for permission to issue stablecoins on privacy-preserving chains. This is a bad bargain for Americans and Treasury should reject it.

A universal view-key—an escrowed capability to decrypt all transactions—is the digital equivalent of installing a microphone in every living room. It cannot be reconciled with America's Fourth Amendment right against warrantless search and seizure or with basic cybersecurity hygiene.

Constitutionally, a universal backdoor amounts to warrantless mass surveillance in violation of Americans' Fourth Amendment rights. Some may argue that the Fourth Amendment does not protect such data because customers have "voluntarily" provided it to a third party, invoking the third-party doctrine to excuse a warrant requirement. That argument misapplies the doctrine. A stablecoin issuer with a view key possesses the ability to expose intimate transactional information about two distinct groups: (1) its customers—those to whom it has issued or from whom it has redeemed stablecoins—and (2) non-customers—individuals who have received or transacted with those stablecoins downstream but who have never had any relationship with the issuer. The third-party doctrine, even if applicable to the first category, cannot constitutionally justify surveillance of the second. It has never permitted, and cannot permit, a deputized intermediary to spy on the private affairs of people with whom it has no business or fiduciary relationship. These people have never voluntarily provided their information to the issuer and the issuer has no legitimate business purpose to obtain non-customer information.[16] To claim otherwise would be to suggest that a car manufacturer or dealership must install tracking devices in every vehicle so that law enforcement can monitor not only the car purchaser's movements but also those of every subsequent driver.

[16]As Coin Center has explained, "[i]f users do not voluntarily hand [transactional] information to a third party … then they logically retain a reasonable expectation of privacy over their personal records, and a warrant would be required …" Peter Van Valkenburgh, Electronic Cash, Decentralized Exchange, and the Constitution 13 (Coin Center Mar. 2019), https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf.

Technically, such systems are brittle and insecure: any compromise of the master key compromises the privacy of every user. Politically, they are untenable: they create the same centralized chokepoint that privacy-preserving blockchains were designed to avoid. A government-mandated view-key architecture would invite constant mission creep, from targeted AML access to generalized domestic monitoring, politically targeted debanking, and—should keys leak (which they always do)—a national security crisis as criminals and foreign actors obtain near perfect visibility into the day-to-day transactions of ordinary Americans. Make no mistake, a stablecoin issued on a privacy-preserving blockchain using a universal view key available to the government creates all the same risks to human liberty as a central bank digital currency.[17] Those who oppose one should also oppose the other.

Treasury should therefore reject any proposal that enables universal, unbounded decryption of user activity on-chain. The proper goal is not omniscience but *assurance*: the ability to verify compliance without exposing private data.

IV. Freeze and Seize Powers, Warrants, and the Danger of False Positives and Political Abuse

The same constitutional principles that forbid warrantless surveillance also constrain warrantless seizure. The GENIUS Act explicitly contemplates "freeze and seize" authority for stablecoin issuers,[18] making it essential to consider these powers through the same constitutional lens applied above. A universal view key would expose Americans' private transactions to government inspection without probable cause; a freeze or block order applied to those same transactions would deprive them of property without judicial process. Both actions offend the Fourth Amendment's core guarantee that searches and seizures of a person's "papers and effects" must be reasonable and supported by a warrant. The distinction between

[17] "If not designed to be open, permissionless, and private — resembling cash — a government-issued CBDC is nothing more than an Orwellian surveillance tool that would be used to erode the American way of life." Majority Whip Tom Emmer, Majority Whip Tom Emmer Reintroduces Landmark Legislation to Protect Americans' Financial Privacy (Feb. 22, 2023), https://emmer.house.gov/media-center/press-releases/majority-whip-tom-emmer-reintroduces-landmark-legislation-to-protect-americans-financial-privacy. "If government officials want someone's information, they must find the right financial institution … Introducing a CBDC could very well serve to close that gap and unleash financial surveillance from its few remaining limitations." Nicholas Anthony, CBDC Spells Doom for Financial Privacy, Cato Institute: Free Society (Fall 2024), https://www.cato.org/free-society/fall-2024/cbdc-spells-doom-financial-privacy.

[18] See U.S. Senate Comm. on Banking, Hous. & Urban Affs., Myths vs. Facts: The GENIUS Act 2 (May 8, 2025), https://www.banking.senate.gov/imo/media/doc/myths_v_facts_-_genius_act_5_8_25pdf.pdf ("The GENIUS Act requires all stablecoin issuers, including foreign issuers, to have the technological capability to freeze and seize stablecoins and also comply with lawful orders.").

observing an otherwise encrypted ledger and freezing an American's assets at some address is one of degree, not of kind—each is a governmental intrusion upon protected rights.

The Constitution's Fourth Amendment squarely prohibits the government from seizing the property of Americans without a warrant issued upon probable cause. A freeze or block order over digital assets in a wallet is no different from the physical seizure of cash or real property. The Supreme Court has long held that "a seizure of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[19] When Treasury or any other U.S. authority directs a financial intermediary or issuer to freeze an American's assets, it has effected precisely that interference. Even when motivated by national security or foreign policy concerns, such actions remain subject to the warrant requirement. As the Court has emphasized "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillance may be conducted solely within the discretion of the Executive Branch."[20] This legal analysis is straightforward. The specific fact pattern of an American's assets being blocked by sanctions and a claim of Fourth Amendment protection being made is, nonetheless, underlitigated at present. In the most recent case on point, a federal district court found that sanctioning the assets of an American nonprofit *did* qualify as an unreasonable seizure under the Fourth Amendment: "Given the substantial intrusion on KindHearts' interest, the seizure here was not reasonable under the Fourth Amendment based on the totality of the circumstances."[21] Given the recent uptick in stablecoin usage and the clear legislative call for freeze and seize powers in GENIUS, we anticipate much further litigation on the topic, and expect that many courts will validate the right of Americans to be free from warrantless seizure of their stablecoins.

Independent of the Constitution's procedural safeguards, sanctions law itself imposes a substantive limit on Treasury's authority. The International Emergency Economic Powers Act (IEEPA) empowers the President to regulate or block "transactions involving any property in which any foreign country or a national thereof has any interest."[22] The statute's reach ends there: it does not authorize the freezing of purely domestic assets or the sanctioning of U.S. persons.[23] In Van Loon v. Department of Treasury, the court recognized this textual boundary,

---

[19] United States v. Jacobsen, 466 U.S. 109, 113 (1984)

[20] United States v. United States Dist. Ct. (Keith), 407 U.S. 297, 317 (1972).

[21] KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner, 647 F. Supp. 2d 857, 908 (N.D. Ohio 2009); see also Peter Van Valkenburgh, When Does a Sanction Become a Seizure? Lessons from the KindHearts Case, Coin Center (May 7, 2019), https://www.coincenter.org/when-does-a-sanction-become-a-seizure-lessons-from-the-kindhearts-case/.

[22] 50 U.S.C. § 1702(a)(1)(B) (2022).

[23] See Van Loon v. Dep't of Treasury, No. 6:23-cv-00508, slip op. at 21–22 (W.D. Tex. Aug. 17, 2023) (holding that IEEPA "does not grant OFAC authority to regulate or block transactions between U.S.

holding that OFAC exceeded its authority when it applied IEEPA sanctions to an American's use of a smart contract in a wholly domestic context.[24] Extending IEEPA to reach Americans' private property or purely domestic transactions would not only contradict Congress's plain intent but would also raise grave constitutional questions under the Fourth and Fifth Amendments.

Treasury's authority under Section 311 of the USA PATRIOT Act likewise extends only to foreign jurisdictions, institutions, and classes of transactions that pose a primary money-laundering concern.[25] It does not authorize the imposition of special recordkeeping or blocking measures on purely domestic activity. Accordingly, to the extent Treasury relies on its Section 311 powers in the context of stablecoins, that authority cannot lawfully be applied to transactions that occur wholly within the United States or between U.S. persons. Extending it further would exceed Congress's express intent and duplicate the same constitutional infirmities that arise under IEEPA.

Together, these limits form a coherent principle. The Fourth Amendment dictates *how* the government may seize property—it must do so only with a warrant supported by probable cause. IEEPA and Section 311 define *what* property may be seized—it must be foreign, not domestic. A warrantless freeze or block of a U.S. person's stablecoins therefore violates both doctrines: procedurally, because it is a warrantless seizure; and substantively, because it targets property Congress never authorized Treasury to reach. Respecting these boundaries is not an impediment to effective sanctions policy—it is what preserves the rule of law even in matters of national security.

These limitations also create difficult administrative challenges for regulated stablecoin issuers. An issuer may be obligated to freeze the assets of a foreign person when directed by lawful sanctions authorities, yet it must also refuse any unconstitutional or mistaken warrantless order to freeze the assets of an American. Because issuers will not always know the nationality of a stablecoin holder—particularly when that person is not their customer—compliance

---

persons occurring wholly within the United States"); 50 U.S.C. § 1702(a)(1)(B) (2022) (limiting the President's blocking authority to transactions involving "any property in which any foreign country or a national thereof has any interest").

[24] *Id.*

[25] See 31 U.S.C. § 5318A(a)(1) (2022) (authorizing the Secretary to impose "special measures" only when a jurisdiction, financial institution, class of transactions, or type of account is found to be "of primary money laundering concern" and specifying that such measures may be applied only with respect to "foreign jurisdictions, foreign financial institutions, [and] classes of transactions involving a foreign jurisdiction or foreign financial institution"); see also Special Measures Imposed Against Foreign Jurisdictions, Foreign Financial Institutions, or International Transactions of Primary Money Laundering Concern, 68 Fed. Reg. 35,548 (June 13, 2003) (codifying FinCEN's interpretation that § 311 "provides the Secretary with a range of options to address specific foreign threats to the U.S. financial system").

becomes fraught with risk. Fortunately, the very technologies about which Treasury now seeks comment may help resolve this dilemma.

V. Constructive Path Forward: Privacy-Preserving Compliance and Due-Process-Respecting Controls

Coin Center supports the development of verifiable, privacy-preserving digital identity tools capable of meeting legitimate regulatory objectives without resorting to mass surveillance. The technologies to achieve this balance already exist. Developing and deploying them, however, is a public good—one that the private sector cannot be expected to pursue on its own. Regulated financial institutions often have limited incentive to lead such efforts. Many benefit from the customer lock-in created by traditional, manual onboarding processes and understandably fear regulatory scrutiny if they experiment with newer methods that lack an established compliance pedigree. As a result, innovation that could strengthen both privacy and oversight risks stagnating unless Treasury explicitly encourages and protects responsible experimentation.

In the context of stablecoins, Coin Center urges Treasury to consider two key directions for that experimentation:

1. **Alternative customer onboarding** at regulated entities using verifiable digital credentials and privacy-preserving identity techniques; and

2. **Smart-contract–mediated freeze controls** designed to rapidly correct obvious false positives and preserve due process within any freeze-and-seize regime.

We recognize that this Advance Notice of Proposed Rulemaking marks only the beginning of Treasury's policy development in this area. Accordingly, we offer these proposals at a high level, with the goal of informing and inspiring future rulemaking, pilot programs, and collaborative research.

Before describing potential technological paths forward, it is important to clarify the scope of these proposals. The discussion that follows concerns the obligations of regulated financial institutions—specifically, permitted payment-stablecoin issuers and custodial intermediaries such as exchanges and "hosted wallet" providers (together money services businesses under existing law and guidance)—in their direct relationships with customers. Nothing here should be read to suggest that Bank Secrecy Act or Customer Identification Program requirements should extend to individuals who use self-hosted wallets or who transact peer-to-peer without an intermediary including using stablecoins. The BSA governs financial institutions, not private persons acting on their own behalf. Only in the limited context of sanctions enforcement—where lawful blocking or seizure orders under IEEPA or Section 311 of the USA

PATRIOT Act may apply—do regulated entities bear obligations touching non-customer transactions, and even then such orders must be constitutionally and statutorily constrained. They cannot be applied to U.S. persons or to purely domestic transactions without a warrant and probable cause. With that boundary in place, the following subsections outline two areas where Treasury could safely foster innovation while respecting those limits.

1. Alternative Onboarding and Risk-Scoring.

Customer onboarding under the current Bank Secrecy Act regime is duplicative, intrusive, and poorly suited to the realities of modern digital systems. Every financial institution must independently collect, verify, and store extensive personal information—names, addresses, Social Security numbers, and identification documents—even when other regulated entities have already completed equivalent checks.[26] This practice offers little additional security but multiplies privacy risk and compliance cost.

As Coin Center's report *Tear Down This Walled Garden* explains, novel AML systems may meet policy goals while collecting far less personal data. "What regulators usually need to know is not who you are, but whether you are permitted to engage in a specific kind of transaction."[27] We argue that future onboarding should therefore become (1) *portable*—allowing customers to reuse verified credentials across institutions; (2) *attribute-based*—disclosing only those facts relevant to compliance; and (3) *dynamically risk-scored*—enabling regulated entities to rely on some public process of aggregating verifiable credentials into a dynamic risk score rather than performing that process opaquelly and independently. Each step progressively reduces unnecessary data collection while improving auditability and privacy.

Stage One: Portable Onboarding.

In the near term, Treasury should encourage the use of portable digital identity credentials that allow customers to reuse verified identity information across institutions. Today, every financial intermediary must separately collect and store the same personally identifying information, even when a user's identity has already been verified elsewhere. This duplication provides no additional assurance and instead multiplies privacy risk. A portable system would allow a user who has already completed high-assurance identity proofing to present a cryptographically verifiable credential to any regulated entity without repeating the entire onboarding process.

[26] 31 C.F.R. § 1020.220(a)(2)
[27] Peter Van Valkenburgh & Ian Miers, Tear Down This Walled Garden: American Values and Digital Identity 9 (Coin Center 2025)

The appropriate benchmark for such credentials is NIST Identity Assurance Level 2 (IAL2),[28] which defines the strength of the identity proofing that occurs before a credential is issued. Under IAL2, the user's identity must be verified through validated documents and authoritative record checks, then cryptographically bound to a digital credential. The credential must also incorporate liveness and proof-of-possession controls to ensure that it is being used by the legitimate, live person who was originally proofed and not by a thief or an automated agent.

Treasury should make clear that a credential issued following an IAL2-compliant process satisfies FinCEN's requirement that a financial institution "form a reasonable belief that it knows the true identity of each customer."[29] When a stablecoin issuer or custodial intermediary verifies such a credential's signature, revocation status, and proof of control by the live credential holder, it achieves equivalent or superior assurance compared with traditional CIP methods, while avoiding redundant collection and storage of sensitive personal data. Stablecoin issuers and custodial intermediaries should also be permitted, if they choose, to serve as credential issuers themselves, provided that their proofing processes meet IAL2 standards and remain subject to audit. Allowing regulated financial institutions to issue credentials directly would promote competition and interoperability in digital identity markets while preserving accountability and consumer protection.

By making customer identity portable, Treasury would modernize CIP without weakening it. A portable, verifiable credential system would strengthen compliance assurance, reduce user friction, and sharply limit the unnecessary spread of personal information across the financial system. It is the first practical step toward a digital identity infrastructure that is both effective and privacy-preserving.

Stage Two: Attribute-Based Onboarding.

Once confidence in credential authenticity and interoperability is established, Treasury should permit stablecoin issuers and custodial intermediaries to rely on attribute-based proofs rather than full identity disclosure. In this model, credentials would reveal only the specific attributes relevant to compliance—such as "U.S. person," "not on the OFAC list," or "identity verified at or above IAL2"—while omitting personally identifying details. The regulated entity's obligation would shift from collecting and storing identity data to verifying the validity and provenance of credentials. This transition preserves compliance assurance while sharply reducing privacy risk, data retention burdens, and the systemic vulnerabilities associated with centralized identity databases.

---

[28] See NIST, Digital Identity Guidelines (SP 800-63-3) §§ 4.4–4.5 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.
[29] 31 C.F.R. § 1020.220(a)(2)

Crucially, attribute-based onboarding would entail a meaningful but necessary reframing of the "know your customer" concept. The regulated entity would still "know" that its customers are legitimate and compliant, but it would no longer know who they are in the traditional, dossier-building sense. Verification would occur through cryptographic proofs and attestations rather than through the possession of personal identifiers. As we have written "A financial institution may have a good business reason to know certain specific risks a customer presents (creditworthiness, illicit activities). That does not mean they have a good business reason to know anything else about them. Indeed, in a free society, we should actively seek to deprive financial institutions of any knowledge of our politics, race, sexual preferences, religion, speech activities, etc."[30] This step is both technically feasible and philosophically consistent with long-standing U.S. privacy norms: the government's legitimate interest is in compliance, not omniscience.

Stage Three: Dynamic Risk Scoring.

Ultimately, onboarding could evolve toward dynamic, on-chain risk-scoring systems that align compliance assurance with measurable indicators of trust rather than static identity records. A neutral oracle or smart contract could aggregate multiple credential attestations and behavioral proofs—such as liveness checks, wallet longevity, transaction history, or credential freshness—to produce a composite compliance score. That score would represent the outcome of many independent verifications, none of which requires disclosing underlying personal data.

Users would retain control over which credentials to disclose to improve their score, and regulators could audit the scoring algorithms and parameters themselves rather than surveilling individual transactions. This inversion—verifying the rules instead of the people—achieves oversight without dragnet monitoring. A wallet's compliance posture would become transparent and auditable, even as the identity of its owner remains private.

For practical purposes, a user who wishes to engage with a stablecoin issuer or custodial intermediary in what would traditionally be a "customer relationship" could present their risk score as the sole credential required for service, in this case issuance or redemption of a stablecoin. The stablecoin issuer's AML obligation would thus be satisfied by issuing to or redeeming from only those wallets whose scores exceed a defined regulatory threshold. The issuer would never need to surveil or collect intimate data from any person. Such a system is both more precise and less invasive than traditional KYC: it rewards good actors with frictionless access while automatically deterring high-risk behavior.

[30] Peter Van Valkenburgh & Ian Miers, Tear Down This Walled Garden: American Values and Digital Identity 10 (Coin Center 2025).

These innovations, however, raise important questions for Treasury and FinCEN. What is the agency's actual enforcement objective—*deterrence* through robust credential verification and risk scoring, or *traceability* that allows direct identification of specific users by law enforcement? If the former, these fully anonymous risk-based methods should suffice, indeed they would likely vastly outperform the existing, easy to evade, deterrence effect of manual identification using traditional and easy to fabricate paper credentials. Anonymous deterrence would also be a tremendous boon to privacy, liberty, and American ideals.

If the latter objective—tracing—is the goal, then the questions are *under what due process* and *via which technical process* should correlation between credential data and issuer data be permitted? In other words, how possible should it be to link or reintegrate some proof of attributes on-chain with actual identity documentation collected and held by the original credential issuer? Cryptographic methods can—and should—achieve strong unlinkability through one-time credentials, zero-knowledge proofs, and other methods. Preventing linkability is what prevents these systems from otherwise reverting into panopticons of complete surveillance and control. When, if ever, should the technical need to prevent linkability give way to law enforcement's need for traceability? If linkability is essential can it be designed in a way that prevents abuse; e.g. by dividing the authority to link amongst various parties who will respond only to proper due process (i.e. a search warrant)? When is it more important for the state to identify the people transacting than it is to simply deter bad transactions? To the greatest extent possible, Treasury should work to clarify which of these outcomes, deterrence or traceability, it seeks in specific contexts so that system designers can align architectures with clearly defined regulatory goals.

Policy implementation for early stages of this transition—such as credential portability—is straightforward under existing authority. Section 5318(a)(7) of the Bank Secrecy Act authorizes the Secretary to "prescribe an appropriate exemption" from the Act's requirements when consistent with its purposes.[31] Treasury could invoke that authority to establish a pilot or regulatory sandbox allowing regulated entities to satisfy CIP obligations using IAL2-attested verifiable credentials. Participants could be evaluated on measurable outcomes such as reduced false positives, faster onboarding, and demonstrable privacy gains.

2. Smart-Contract-Mediated Freeze Controls.

The GENIUS Act calls on permitted payment-stablecoin issuers to maintain the technological capability to freeze and seize stablecoins and comply with lawful orders, importing traditional

[31] 31 U.S.C. § 5318(a)(7); 31 C.F.R. § 1010.970 (authorizing the Secretary of the Treasury, acting through FinCEN, to exempt any person, class of persons, transaction, or class of transactions from BSA requirements by regulation or written order).

sanctions-compliance obligations into new environments, blockchains, that are transparent, instantaneous, and global by default.[32] Absent clear guardrails, a freeze function on an open blockchain could easily become a tool for extrajudicial control or political abuse. The unique programmability of stablecoins therefore demands a correspondingly precise legal and technical framework—one that upholds legitimate enforcement while preventing unconstitutional seizure and mission creep.

As discussed above, the Constitution and Congress have already defined these boundaries. The Fourth Amendment prohibits the government from seizing the property of Americans without a warrant supported by probable cause. A freeze or block order over digital assets is precisely such an interference, and therefore a seizure. Even when motivated by national-security concerns, these actions remain subject to the warrant requirement.[33] Statutorily, the International Emergency Economic Powers Act (IEEPA) empowers the President to block "transactions involving any property in which any foreign country or a national thereof has any interest."[34] Its reach does not extend to the property of U.S. persons or to purely domestic transactions.[35] Likewise, Section 311 of the USA PATRIOT Act applies only to "foreign jurisdictions, foreign financial institutions, or transactions involving a foreign jurisdiction or foreign financial institution."[36] These limitations are not technicalities—they are essential safeguards. The Fourth Amendment governs *how* property may be seized, and IEEPA and § 311 define *what* property may be targeted.

These constraints, while constitutionally vital, create genuine administrative challenges for regulated stablecoin issuers. An issuer may be obligated to freeze the assets of a sanctioned foreign person but must also refuse any unconstitutional or mistaken order to freeze the assets of an American. Yet issuers may not always know the nationality of a wallet holder who is not their customer. Acting incorrectly in either direction carries risk: failure to freeze may expose the issuer to enforcement; freezing an American's assets without a warrant may constitute a constitutional violation. The dilemma is not whether issuers should comply with lawful sanctions—they must—but how they can do so in a way that is accurate, auditable, and rights-respecting.

Much of this will likely end up hashed out in court cases, as inevitable false positive freezes will lead to Americans' challenging freeze orders in court. This will be a necessary but also costly, slow and wasteful process. Is there a way to address some false positives more efficiently?

---

[32] See U.S. Senate Comm. on Banking, Hous. & Urban Affs., Myths vs. Facts: The GENIUS Act 2 (May 8, 2025),
[33] See United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297, 316–17 (1972)
[34] 50 U.S.C. § 1702(a)(1)(B).
[35] Van Loon v. Dep't of Treasury, No. 6:23-cv-00508 (W.D. Tex. Aug. 17, 2023).
[36] 31 U.S.C. § 5318A(a)(1).

A solution may lie in rule-based, transparent automation: smart-contract–mediated enforcement. A well-designed stablecoin contract could implement "freeze" and "unfreeze" logic transparently, using verifiable cryptographic rules and strict limits on discretionary human action. An issuer could flag specific tokens as frozen only upon presentation of a valid OFAC order or court warrant. The parameters of the order—scope, target address, and duration—could be logged on-chain for transparency and audit. The same contract could include an unfreeze function to protect against false-positives and grant victims with overwhelming evidence of innocence a quick way out. It could enable the affected wallet to present cryptographic proof of U.S. personhood using composable verifiable credentials and zero-knowledge proofs. If the proof meets an established risk-score threshold—for example, combining a mobile driver's-license credential, a bank-grade KYC credential, and a liveness signal—the contract could automatically release the funds. All such actions could be immutably recorded, providing accountability without exposing personal information.

We recognize that this sketch of a proposal demands significant investigation before it could become viable. National security concerns or the need to maintain investigative secrecy may make the degree of transparency suggested here difficult in practice. Similarly, the complications inherent in proving that one's funds should be unfrozen are substantial. What if a user is an American, yet the government claims that the targeted property is jointly held, off-chain, with foreign persons or entities? Is there a zero-knowledge proof of *nonforeign interest* that would be both technically sound and legally sufficient? Questions such as these demonstrate that further research—technical, legal, and institutional—is essential before any automated freeze and unfreeze system can be responsibly deployed.

Nevertheless, this is an area where sustained work is urgently needed. False positives in sanctions enforcement are real, and as stablecoins become more widely used by ordinary Americans for payments, the implications for liberty and financial inclusion will be profound. Indeed, if issuers retain unbound technical capacity to block and freeze stablecoins and if governments can pressure them to exercise that authority unilaterally, secretly, and without public and judicial scrutiny, then this technology is far from Bitcoin or similar innovations. Stablecoins would become a trap rather than a shield for Americans seeking to protect and exercise their rights. Treasury should therefore treat this as a research and pilot priority: to explore how programmable compliance tools might codify due process into enforcement mechanisms, protecting both the state's legitimate interest in sanctions enforcement and the individual's constitutional right to property and fair process.

A smart-contract freeze regime built on verifiable credentials would not be a panacea, but it could be a step toward reconciling enforcement with constitutionalism. Properly designed, it could isolate enforcement to intended targets, leave a permanent audit trail, protect personal

data from misuse, and restore to individuals a meaningful way to challenge mistaken seizures. The challenge for Treasury is to ensure that the technological capability to freeze and seize, as contemplated by the GENIUS Act, becomes a *capability to protect rights as well as enforce law.*

VI. Conclusion

As this comment explains, naively grafting legacy, identity-heavy AML practices onto public ledgers would create a panopticon that is both unconstitutional and unamerican. The better path is privacy-by-design: (1) issuing stablecoins on privacy-preserving networks and allowing stablecoin holders to utilize privacy preserving smart contracts on otherwise public networks; (2) replacing bulk identity collection at regulated issuers with portable, IAL2-proofed credentials and attribute-based verification, and (3) exploring rule-based, auditable automation to cabin freeze authority and provide due-process remedies for false positives—especially where U.S. persons' property is at stake.

To that end, Treasury should take the following actions:

1. Affirm constitutional and statutory limits. Make clear that freezes of U.S. persons' assets require a warrant supported by probable cause, and that IEEPA and 311 authorities apply only to foreign property/transasctions/interests—and not purely domestic transactions or Americans' property.
2. Support privacy-preserving issuance and reject universal view-key mandates. State that stablecoin issuance on privacy-preserving blockchains is consistent with the BSA. State that stablecoin holders can lawfully use privacy-preserving smart contracts and tools. Clarify that architectures enabling unbounded decryption of user activity are incompatible with the Bank Secrecy Act's purpose and Americans' Fourth Amendment rights.
3. Establish a targeted pilot program for issuers under BSA exemptive authority. Using 31 U.S.C. § 5318(a)(6), create a safe harbor for portable, IAL2-proofed verifiable credentials that satisfy CIP's "reasonable belief" standard without duplicative PII collection; permit regulated issuers/custodians to serve as credential issuers subject to audit.
4. Convene a *Future of AML Standards* track. In coordination with NIST and relevant stakeholders, solicit proposals for (A) alternative attribute-based onboarding and dynamic risk scoring, and (B) smart-contract-mediated freeze/unfreeze controls with documented assurance levels, transparency features, and appeal mechanisms.

Coin Center has recently begun work on The John Hancock Project, a small stakeholder group composed of privacy-focused technologists, civil liberties advocates, and academic experts. The JHP intends to develop implementable open standards for decentralized, maximally

privacy-preserving identity credential architecture. We hope the JHP can be a lab to work on alternative AML and identity technologies that are true public goods, otherwise underproduced by the private sector. The more speculative proposals in this comment—dynamic on-chain risk scoring and smart-contract mediated freeze/unfreeze controls—will require much further development before implementation, but Treasury is not alone, the JHP is here to help.

Treasury's charge under the GENIUS Act is to foster integrity and innovation. The roadmap above does both: it strengthens enforcement where it matters, reduces systemic risk from unnecessary data hoards, and protects the constitutional freedoms that make open financial systems worth building. We thank you for engaging in this process and welcome further conversations.

Sincerely,

Peter Van Valkenburgh

Executive Director of Coin Center