ANDREESSEN
HOROWITZ

October 17, 2025

BY ELECTRONIC SUBMISSION

Julie Lascar
Director
Office of Strategic Policy, Terrorist Financing and Financial Crimes
U.S. Department of the Treasury
1500 Pennsylvania Ave., NW
Washington, DC 20220
innovationdigitalassetsrfc@treasury.gov

Re: Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets (ID TREAS-DO-2025-0070-0001)

Dear Ms. Lascar:

Andreessen Horowitz ("a16z") appreciates the opportunity to respond to the Department of the Treasury's (the "Department" or "Treasury") request for comment, dated August 18, 2025 (the "Request"), on the use of innovative or novel methods, techniques, or strategies to detect and mitigate illicit finance risks involving digital assets.[1] We appreciate the Department's commitment to fulfilling the requirements of the Guiding and Establishing National Innovation for U.S. Stablecoins ("GENIUS") Act and supporting the Administration's policy of supporting the responsible growth and use of digital assets, blockchain technology, and related technologies, as provided in President Trump's Executive Order 14178.[2]

I. About a16z

A16z is a venture capital firm that invests in seed, venture, and late-stage technology companies, focused on bio and healthcare, consumer, crypto, enterprise, fintech, and games. A16z currently has more than $74 billion in committed capital under management across multiple funds, with more than $7.6 billion in crypto funds. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch Internet businesses. Our funds typically have a 10-year time horizon, as we take a long-term view of our investments, and we do not speculate in short-term crypto-asset price fluctuations.

II. Executive Summary

The GENIUS Act is a momentous step in advancing the future of digital finance and integrating blockchain systems into traditional markets. We believe that the Act will foster responsible innovation and unlock the benefits of blockchain technology, and we agree with the

[1] Treas. Dep't, *Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets*, 90 Fed. Reg. 40,148 (Aug. 18, 2025), https://www.regulations.gov/document/TREAS-DO-2025-0070-0001.
[2] Exec. Order 14178, 90 FR 8647 (Jan. 31, 2025); GENIUS Act, Public Law 119–27, 139 Stat. 419, at Sec. 9(a).

Department that it will strengthen the U.S. dollar's reserve currency status and bolster U.S. national security while prioritizing consumer protection. Importantly, the GENIUS Act also seeks to counter illicit finance, including through its requirement that the Secretary seek public comment on four specific technologies for mitigating illicit finance risk involving digital assets: application program interfaces (APIs), artificial intelligence (AI), digital identity verification, and use of blockchain technology and monitoring.[3] We look forward to collaborating with the Department as it explores these tools in this Request and implements other provisions of the Act.

A16z is deeply committed to thought leadership and supporting technological innovation regarding each of the topics outlined in the Request. To that end, we welcome any invitation to engage with Treasury and the law enforcement community to discuss any of these important issues. In this comment letter, we have chosen to focus on "digital identity verification," particularly on Questions 4(c)-(e) of the Request, because we believe that our experience is most directly relevant to these topics. As artificial intelligence advances, challenges such as deepfakes and digital fraud will proliferate, making it imperative to develop digital identity solutions that are able to verify that an individual is human and, in fact, who they claim to be. As is reflected in our investments, we are thus committed to the development of robust and privacy-preserving digital identity solutions. We have led funding rounds and invested in:

- Spruce Systems,[4] a digital identity startup that builds open-source tools that help users collect, control, and own their data across the internet;[5] and

- World,[6] which consists of a privacy-preserving digital identity network (World ID) capable of establishing that an individual is both human and unique;[7]

We also understand and appreciate the significant privacy concerns that can arise from the proliferation of digital identity, including the potential for surveillance. For that reason, and as discussed below, we are highly supportive of the use of zero-knowledge proofs (ZKPs) and other privacy tools to mitigate these concerns. In addition, we have also invested in privacy protocols, which make it more difficult for adversaries of the United States, such as China and Russia, to steal and exploit the personal data of American citizens and businesses, while also enabling law enforcement agencies and the intelligence community to enforce the law and perform their critical functions.[8]

---

[3] GENIUS Act, Public Law 119–27, 139 Stat. 419, at Sec. 9(a).
[4] SpruceID, https://spruceid.com/.
[5] Eddy Lazzarin & Chris Dixon, *Investing in Spruce*, Andreessen Horowitz (Apr. 21, 2022), https://a16z.com/2022/04/21/investing-in-spruce/; A list of investments made by a16z managed funds is available at https://a16z.com/investments/.
[6] World, https://world.org/.
[7] *World raises $135M from Andreessen Horowitz and Bain Capital Crypto to fund network expansion*, World (May 21, 2025), https://world.org/blog/announcements/world-raises-135m.
[8] We have also invested in Aztec, which integrated into its testnet ZKPassport, an open-source, permissionless, and self-custodial digital-identity system that leverages the same International Civil Aviation Organization open standards infrastructure used globally in airports and national border systems to authenticate electronic identity documents. ZKPassport, https://zkpassport.id/; David Steinrueck, *ZKPassport Case Study: A Look into Online Identity Verification*, Aztec (June 26, 2025),

We particularly believe that the use of decentralized digital identity can dramatically change how individuals go about their everyday lives; how businesses can fulfill their regulatory obligations; and how law enforcement and the intelligence community can fulfill their important missions. With the proper regulatory approach, which includes strict privacy-protecting standards, the United States has a unique opportunity to lead the world in ensuring a robust digital identity ecosystem that strengthens privacy protections for individual Americans, while reducing compliance burdens for businesses *and* bolstering the ability of law enforcement to protect the public against cybersecurity incidents and illicit finance risks.

III. Background on digital identity

Americans need identification for all sorts of everyday activities, including opening a bank account and driving a car. The different types of digital identity archetypes are commonly categorized in three ways: centralized, federated, and decentralized.[9] Today, centralized and federated identities predominate, while decentralized digital identity has emerged as an important potential paradigm shift.[10]

- **Centralized/Federated**: Centralized identity systems are platforms created and managed by centralized parties such as governments, financial institutions, and others. In federated identity systems, identity providers operate as a network or "federation" of organizations; each participating organization manages its own stand-alone system, which interoperates with the systems of other participating organizations. In this model, third-party providers generate credentials for individuals and provide them to other digital services in the network on behalf of an individual. Crucially, both centralized and federated identity systems require an individual to rely on a third party to manage their information. In this way, both intermediate processes involving identification.

- **Decentralized**: Decentralized digital identity refers to an online identity that relies on blockchain technology or other verifiable data registry, where individuals, rather than centralized entities, have full control over their personal data and information.[11] A decentralized digital identity, or "passportable ID," can be issued once, and it enables multiple entities to attest and verify an individual's identity credentials, while

---

https://aztec.network/blog/zkpassport-case-study-a-look-into-online-identity-verification; Ali Yahya & Guy Wuollet, *Investing in Aztec*, a16z crypto (Dec. 15, 2022), https://a16zcrypto.com/posts/article/investing-in-aztec/.

[9] United Nations Joint Staff Pension Fund & United Nations International Computing Centre, *Transforming Public Digital Identity: A Blockchain Case in Action from the UN System*, at 6 (Sept. 2025), https://www.unicc.org/wp-content/uploads/2025/09/UNICCUNJSPF_Transforming-Public-Digital-Identity-2.pdf.

[10] Various standards bodies and government agencies, such as the National Institute of Standards and Technology (NIST), the World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETC), the International Organization for Standardization (ISO), and the OpenID Foundation (OIDF) have researched and promulgated proposed structures for digital identity. In addition, jurisdictions in the United States, such as Utah, and abroad, including in the European Union, are already experimenting with and implementing digital identity verification. *See, e.g.*, Wayne Chang, *Utah's Digital ID Bill SB260 is the New Frontier for User-Controlled Identity*, SpruceID (Mar. 11, 2025), https://blog.spruceid.com/utahs-digital-id-law-sb260-is-the-new-frontier-for-user-controlled-identity/.

[11] Coinbase Institute, *Primer: Decentralized Identity*, https://www.coinbase.com/public-policy/advocacy/documents/decentralized-identity.

empowering the user to control their personal data. Importantly, using blockchains and cryptographic techniques, such as ZKPs, users also determine how much of their personal information they are comfortable sharing with others, as well as with whom that information is shared.[12]

Decentralized identity systems can operate in different ways, including through decentralized identifiers ("DIDs") and verifiable digital credentials ("VDCs").

- A DID is a unique ID that acts as "proof of ownership" over a digital identity of a subject, i.e., a person, organization, or thing. DIDs point to "DID documents," which contain information explaining how to use the DID, such as a verification method. Using the information recorded in the DID document, participants can verify a proof made by the DID subject, authenticating that the subject owns a particular digital identity.[13] A key feature of DIDs is that they are user-controlled authenticators—managed by their holder rather than a third party.

- VDCs are cryptographically-secured digital records that allow issuers to make verifiable attestations about an individual, while making it possible for verifiers to authenticate this information without relying on intermediaries.[14] For example, a bank could attest to a person's account history or a university could attest to a degree. VDCs are stored in a user's wallet, and can be associated with a DID. A person can then present proofs regarding their credentials to satisfy a verifier's requirements.[15]

An individual can use decentralized identity systems to selectively prove personal information about themselves to others, such as their age, birthdate, or citizenship. In this way, such systems provide a mechanism by which verifiers in a network can authenticate the truth of an individual's claims without exposing their identity. An individual can make these verifiable claims across many online platforms and services. In addition, the verifier of the information, e.g., a financial institution, can check the provenance of the credential without having to connect with the original issuer.

Although centralized/federated digital identity solutions are currently more pervasive, decentralized identity solutions are far superior for both United States law enforcement and U.S. citizens. Because centralized/federated identity approaches require intermediaries, the systems themselves are less resilient, subject to cyber-attacks and other intrusions at their weakest point of entry. Those intermediaries sometimes also conduct rent-seeking on their users, making consumers dependent upon them in exchange for providing such basic—albeit critical—services as proof of identity. And finally, for the same reasons that central bank digital currencies are

---

[12] Robert Stevens, *What Is Decentralized Identity?*, CoinDesk (Mar. 24, 2023), https://www.coindesk.com/learn/what-is-decentralized-identity.
[13] W3C, *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations* (July 19, 2022), https://www.w3.org/TR/did-1.0/.
[14] *Id.*
[15] Importantly, methods exist to help preserve the privacy of individuals using this identity architecture. For example, individuals can generate a new DID for each relationship or interaction, helping to prevent reidentification via correlation across multiple DIDs.

problematic, centralized/federated digital identity solutions risk the privacy and autonomy of their users. As detailed above, decentralized solutions for digital identity allow users to control their data: what gets shared, who it is shared with, and how it is used. Users are allowed to preserve their privacy without reliance—sometimes completely unjustified reliance—on third parties, regardless of whether those third parties are large companies or governments.

IV. Comments in Response to Questions 4(c)-(d)

A. Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Digital identity solutions can offer substantial benefits to individuals, financial institutions, and others in conducting their financial transactions and other day-to-day affairs. Furthermore, digital identity can not only protect, but in fact further, important public interests, including law enforcement interests in combating money laundering, sanctions evasion, and other forms of illicit finance. If implemented properly and designed with sufficient privacy protections, such solutions can empower individuals with control over how their identities are maintained and shared;, they can avoid unnecessary over-sharing with both corporations and governments which can give rise to "surveillance state" issues and government overreach; and they can assist law enforcement and the intelligence community to combat financial crime. But, it is imperative that any digital identity technology include required standards around privacy, lest we unintentionally create tools that could be used for unwarranted and invasive or even dangerous purposes akin to the technology already operating in China.

Unfortunately, existing regulatory and supervisory regimes hamper and discourage the ability of financial institutions to employ emerging technology, including decentralized digital identity solutions, in conducting their BSA/AML compliance programs in connection with customer due diligence, onboarding, reporting of certain financial transactions, information sharing, and other essential components of compliance.

By way of example, existing Customer Identification Program (CIP) rules[16] require many types of financial institutions, including banks and brokers and dealers of securities, to onboard customers via verification of government-issued identification documents. There are certain instances where they may use "non-documentary methods" to verify customers, see, e.g., 31 CFR § 1020.220(a)(ii)(B), and there may also be situations where the bank (or other institution) may rely on other financial institutions to ensure verification of other information by the customer. See, e.g., 31 CFR § 1020.220(a)(6).

While somewhat helpful in allowing banks to complete their compliance obligations, these flexibilities are extremely limited in word and in practice. For example, the "non-documentary methods" exemption and third-party reliance provisions are not available to many types of financial institutions, including money services businesses (MSBs), casinos,

[16] *See* 31 CFR § 1020.220 (banks); 31 CFR § 1023.220 (brokers or dealers in securities); 31 CFR § 1024.220 (mutual funds); 31 CFR § 1026.220 (futures commission merchants and introducing brokers in commodities).

precious metals dealers, and others. In fact, most cryptocurrency exchanges, and other virtual asset service providers, qualify as MSBs, which are not covered by the non-documentary methods rules and third-party reliance allowances.[17]

Furthermore, even if these "exemptions" were comprehensively available across all financial institutions, their reach only goes so far, and not far enough. For instance, neither FinCEN nor any other agency has clarified that any digital identity technologies would satisfy the "non-documentary methods" provisions.[18] And those rules still require that the financial institution's procedures address a host of other situations, such as those in which the customer does not have a government-issued photo ID; or the bank is unfamiliar with the customer-provided documents; or where the account is opened without documents or without the customer appearing in person; or various other situations even after the institution has verified the customer through decentralized identity solutions.

Similarly, the CIP rules for banks (and some but not all other financial institutions) allows the bank to rely on the identity verification of another financial institution.[19] But, like the "non-documentary methods" provisions, these rules are fairly restrictive: the entity on whom reliance is placed must also be a financial institution regulated by another federal functional regulator. And the two financial institutions must abide by a formal contract, which among other things requires annual certification of the existence of an AML program, and that the specific CIP requirements have been or will be performed. Furthermore, in all cases, the rule provides that the financial institution must be sure that its reliance is "reasonable under the circumstances," without any regulatory clarity as to what might make such reliance justifiable or otherwise. In short, these rules provide for marginal flexibility, and only within the existing frameworks and contractual relationships of the "walled garden" of banks and certain other traditional financial institutions.

---

[17] Although the CIP rules do not apply to certain types of financial institutions, such as casinos and MSBs, many of these institutions, before receiving deposited funds, opening an account, or extending credit, must verify the identity of persons using the CIP "examination of a document" method described in 31 CFR § 1010.312. *See, e.g.*, 31 CFR § 1021.410(a) (casinos and card clubs). Other financial institutions are required to examine documents before conducting certain types of financial transactions. *See* 31 CFR § 1010.312.

And apart from these specific, prescriptive rules, all financial institutions are subject to some type of "know-your-customer" requirements to verify customer information. For instance, though not subject to the CIP rules, MSBs are subject to KYC obligations, both generally and in the context of specific transactions. *See, e.g.*, 31 CFR § 1021.210(d)(1)(i)(A) (MSBs required to maintain policies, procedures, and internal controls including provisions for verification of customer information).

For purposes of the requested regulatory relief, those non-bank financial institutions should also be allowed to use decentralized identity solutions, and therefore the exemption should entitle those institutions to use "non-documentary methods" in fulfillment of their KYC requirements and other reporting and recordkeeping obligations.

[18] It is possible to read the CIP provisions to allow a digital identity to be deemed a "document" for purposes of the CIP rule, especially if such a digital identity certificate were issued by the government. *See, e.g.*, 31 CFR § 1022.210(a)(2)(ii)(A). However, the regulation gives an example that "[f]or an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport" which suggest that such digital certificates would not be considered within the expectation of the CIP rule as currently drafted.

[19] 31 CFR § 1020.220(a)(6).

Therefore, many of the existing rules and expectations surrounding CIP and KYC allow for traditional means of identity verification, with slight flexibility at the margins. But some of these flexibilities and exceptions stop well short of what might be needed to (1) foster innovation in technologies that might dramatically improve BSA/AML compliance; (2) allow individuals to maintain and protect their private information; and (3) lead to solutions that assist law enforcement and the intelligence community to combat illicit finance.

Indeed, some of the regulators' own guidance has effectively discouraged the use of innovative ways of satisfying BSA/AML obligations. By way of example, in December 2018, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration, and the Office of the Comptroller of the Currency issued the *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing*.[20] Among other things, the *Joint Statement* acknowledges that banks have considered innovative solutions to combat illicit finance, and provides guidance to those institutions in deciding whether to implement such solutions. The guidance notes that "[s]ome banks are … experimenting with artificial intelligence and digital identity technologies applicable to their BSA/AML compliance programs," and that the regulators "welcome these types of innovative approaches to further efforts to protect the financial system against illicit financial activity."

But although the *Joint Statement* proposes to welcome innovation, the invitation proves hollow. Unfortunately, while well-intentioned, the regulatory guidance makes clear that innovative efforts such as pilot programs have their limits. The pilot programs must be undertaken "in conjunction with existing BSA/AML processes," and financial institutions must continue to operate their existing compliance programs atop their innovative efforts. Neither incentives—nor even reasonable signals or assurances—are in place to allow financial institutions to believe that their efforts would be acceptable to regulators, even if demonstrating a marked improvement in effectively preventing and reporting illicit activity. Instead, many companies are left with the position that even if they in fact develop a better system, they will be forced to continue to operate their duplicative (or sometimes inferior) legacy system in parallel.

It should therefore be unsurprising that many such solutions remain undeveloped, unfunded, and unimplemented. Existing BSA rules and guidance constrain the adoption and development of promising solutions. Simply put, incentives matter. Companies, individuals, and markets all hope to improve their compliance processes, and to assist law enforcement in their mission. But they will only act, and invest, when they rationally believe that their investments in innovation will be worth it (or at the very least, will be permissible in the eyes of the government). And this rationality often leads financial institutions—and their shareholders, investors, and boards—to conclude that investment and deployment of promising innovative solutions will simply not be worth it absent some clear and concrete signal that they will in fact be acceptable to regulators.

---

[20] Available at https://www.fincen.gov/system/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf (Hereafter, "Joint Statement").

B. What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets?

There are opportunities to remedy these obstacles. Certain initiatives by FinCEN and other Treasury components should be continued and expanded, and the government should use its existing authorities, including guidance and exceptive relief, to ensure that decentralized identity solutions and other helpful, innovative technologies can be deployed by financial institutions in aid of BSA/AML compliance. We discuss these recommended steps below.

- **Rescinding the 2018 Joint Statement on Innovation Guidance, and Promulgating a Definite Pathway for Adoption of Innovation Proposals**

Treasury, along with its financial regulatory counterparts, should rescind its *Joint Statement*, and replace this guidance to offer clear, actionable pathways for financial institutions to deploy decentralized identity solutions and other innovations to combat illicit finance. In particular, Treasury (and the other regulators) should establish a clear, definite process whereby a financial institution can establish or implement a program on a pilot basis to test the effectiveness of decentralized identity solutions, with the result of being able to adopt such solutions in satisfaction of its KYC and CIP obligations.

Rather than focusing solely on a some generalized openness to research and experimentation (which, standing alone, does not incentivize innovation), Treasury should offer an opportunity for financial institutions and others to develop solutions which, if proven, can be implemented in practice in satisfaction of the regulatory requirements, without the threat of enforcement or supervisory action. By way of example, a financial institution might develop a method of satisfying regulatory requirements for identity verification and take a series of steps to develop and implement the program:[21] First, the institution drafts a white paper identifying, among other things (1) the regulatory goals it is attempting to meet; (2) if its system/method/technology is effective, the specific regulations it should be deemed to satisfy; and (3) the specific legacy systems/methods/technology the innovation is attempting to replace. Next, both the new and legacy systems are run in parallel for no more than six or nine months to determine the effectiveness of the new system. Third, the new system can be tested by an independent reviewer to determine its effectiveness, and especially to see if it meets the regulatory objectives.

Assuming that the independent review determines that the proposed approach is effective, and meets the underlying purposes of the regulations, then the financial institution will submit the white paper, along with the independent review report, to FinCEN and to the institution's federal functional regulator (if applicable). At this point FinCEN and the functional regulator will have a set amount of time (perhaps six months) to respond. If the functional regulator and FinCEN object to the proposed innovative approach, they must make a specific, articulable

[21] One of the goals of any such proposal should be to preserve user privacy. Accordingly, some additional protections (similar to those found under FCRA or RFPA) are likely necessary to protect such privacy interests, which would prohibit the financial institutions from overcollection for non-BSA (or non-sanctions) purposes or other misuses of the collected information.

objection, outlining how the proposals are not effective, along with specific recommendations as to how to remedy these concerns. Absent such objections, the proposed system may be implemented in lieu of the legacy system and the proposed approach will be deemed permitted, pursuant to FinCEN's exceptive relief authority (and any parallel authorities by other regulators).

The stated purpose of the *Joint Statement* was "to encourage banks to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their Bank Secrecy Act/anti-money laundering (BSA/AML) compliance obligations, in order to further strengthen the financial system against illicit financial activity." But it did not; the *Joint Statement* neither inspired nor incentivized any such innovative approaches to compliance, leaving many financial institutions to run outdated systems that are ill-equipped to handle twenty-first century illicit finance. The government can, and should, rescind and reissue this guidance to allow and incentivize institutions to build effective, safe, and robust systems.

The regulators' examination manuals, which guide examination teams (and inform industry as to the expectations and testing/audit approaches), should be revised to track the shoreline of this reissued guidance.[22]

- **Regulatory Relief**

Although notice-and-comment rulemaking may be appropriate for some changes,[23] FinCEN is already equipped with authority to provide flexibility, allowing for regulatory relief. Pursuant to 31 CFR § 5318(a)(7) and 31 CFR § 1010.970, FinCEN possesses the authority to make appropriate, tailored exceptions to BSA requirements.[24] Indeed, FinCEN has employed exceptive relief in a variety of similar circumstances.[25]

For instance, FinCEN has offered limited exceptive relief regarding the online gaming industry. As described above, although certain types of financial institutions (such as banks) may use "non-documentary methods" to verify customers' identities, other types of financial institutions (such as MSBs and casinos) may not use them under existing regulations. In 2021, after a series of productive engagements with industry and other stakeholders, FinCEN used its

---

[22] The Federal Financial Institutions Examination Council (FFIEC) publishes a Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual to provide guidance to examination teams, and it was developed by both the federal and state banking agencies, along with FinCEN and OFAC. *See* https://bsaaml.ffiec.gov/manual. FinCEN has also published its *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses*, which was last updated in 2008. *See* https://www.fincen.gov/system/files/shared/MSB_Exam_Manual.pdf. Via authority delegated from FinCEN, the Internal Revenue Service, Small Business/Self-Employed Division has examination authority over various non-bank financial institutions, such as casinos, precious metals dealers, and MSBs, that lack a federal functional regulator. Those examination provisions and procedures are set forth in Part 4 of the Internal Revenue Manual. *See* https://www.irs.gov/irm/part4/irm_04-026-009.

[23] Many of the proposals outlined below might be made by notice-and-comment rulemaking to amend the existing regulations, rather than via exceptive relief. For instance, instead of deeming decentralized identity solutions as an exception to the CIP rule, the CIP rule might be explicitly amended to provide for such.

[24] The Exceptive Relief authority has been delegated from the Treasury Secretary to the Director of FinCEN. *See* U.S. Department of the Treasury Order 180-01 (Jan. 14, 2020).

[25] *See also* Peter Van Valkenburgh & Ian Miers, *Tear Down this Walled Garden: American Values and Digital Identity*, Coin Center (Sept. 2025), https://www.coincenter.org/tear-down-this-walled-garden/.

exceptive relief authority to relax its identification rules related to online gaming.[26] Among other things, FinCEN stated that it had learned from industry that online onboarding procedures, "which may include non-documentary identity verification, can provide more comprehensive verification of an online patron's identity than the procedures currently required under FinCEN rules." FinCEN acknowledged that the existing rules "reflect[] technological constraints and legal restrictions that incentivized in-person interaction with customers," but "[t]he gaming industry has since evolved." After considering the equities, especially the technological developments of the industry, FinCEN concluded that exceptive relief was appropriate to allow new business models—and new compliance measures—to exist without strict adherence to the legacy rule.

FinCEN has utilized its discretionary exceptive relief authority under Section 1010.970 to allow persons and industries (classes of persons) in a variety of circumstances, including (1) beneficial ownership reporting requirements for certain rollovers, renewals, and modifications of existing accounts;[27] (2) maintenance of accounts at the Commercial Bank of Syria, in conjunction with the lifting of Treasury sanctions;[28] (3) delaying the effective date of the Investment Adviser Rule;[29] and (4) postponement of AML regulations for residential real estate transfers.[30] In 1998, FinCEN granted exceptive relief regarding the Travel Rule, citing that the agency had "made clear in the past that the purposes of the Travel Rule are not incompatible with flexibility in applying the Rule's literal terms."[31] And on July 31, 2025, the Board of Governors of the Federal Reserve, with the concurrence of FinCEN, granted an exemption regarding the CIP requirement in which the bank may obtain the Taxpayer Identification Number from a third party rather than the customer.[32]

Such flexibility is also warranted here. Use of the exceptive relief authority would recognize that the financial industry has evolved, and, like the relief issued to the online gaming industry in 2021, allowing decentralized identity would "provide more comprehensive verification of [a customer's] identity than the documentary methods currently required by

---

[26] *See* Fin. Crimes Enf't Network, FIN-2021-R001, *Exceptive Relief for Casinos from Certain Customer Identity Verification Requirements* (Oct. 19, 2021), https://www.fincen.gov/system/files/administrative_ruling/2021-10-19/Casino%20Exceptive%20Relief%20101921.pdf.

[27] Fin. Crimes Enf't Network, *Exceptive Relief from Beneficial Ownership Requirements for Legal Entity Customers of Rollovers, Renewals, Modifications, and Extensions of Certain Accounts* (Sept. 7, 2018), https://www.fincen.gov/system/files/administrative_ruling/2018-09-18/Permanent%20Exceptive%20Relief%20Extension%20of%20Compliance%20Date%20CDs_final%20508%202.pdf.

[28] Fin. Crimes Enf't Network, *Exception to Prohibition Imposed by Section 311 of the USA PATRIOT Act against the Commercial Bank of Syria* (May 23, 2025), https://www.fincen.gov/system/files/2025-08/Commercial-Bank-of-Syria-Exceptive-Relief.pdf.

[29] Fin. Crimes Enf't Network, *Exemptive Relief Order to Delay the Effective Date of the Investment Adviser Rule* (Aug. 5, 2025), https://www.fincen.gov/system/files/shared/IA-Rule-Exemptive-Relief-Order.pdf.

[30] Fin. Crimes Enf't Network, *Exemptive Relief Order to Delay the Effective Date of the Residential Real Estate Rule* (Sept. 30, 2025), https://www.fincen.gov/system/files/2025-09/RRE-Rule-Exemptive-Relief-Order-508.pdf.

[31] 63 Fed. Reg. 16, 3640 (Jan. 26, 1998), https://www.govinfo.gov/content/pkg/FR-1998-01-26/html/98-1671.htm.

[32] Bd. of Governors of the Federal Reserve, Order (July 31, 2025), https://www.fincen.gov/system/files/2025-08/CIP-TIN-Exemption-Order-Board-only-508.pdf

FinCEN's regulations."[33] And similar to the Federal Reserve's July 31, 2025 regulatory relief granted to depository institutions for obtaining TIN information, flexibility would be consistent with the purposes of the BSA while also justified because of concerns "relating to consumer privacy and security" as well as "concerns about requirements being burdensome, prohibitively expensive, or impractical."[34] Finally, using Treasury's authority is "[c]onsistent with the Administration's deregulatory policies focused on reducing any unnecessary or duplicative regulatory burden on Americans."[35]

- **Standards for Credentialing**

Assuming that Treasury supports digital identity as a substitute for traditional documents, an important step would be the establishment of standards to onboard customers. Because every state may not have the technological interest or capability to adopt this technology and the need to make it widely available to all residents, there should be multiple options available for individuals to choose from for credentialing, from both the public and private sectors. In addition, pursuant to standards set for such credential issuance, the institutions that onboard traditionally would be able to issue a verified credential based on existing onboarding processes. Other private sector companies may develop technologies and processes to accomplish these tasks, roughly analogous to CLEAR for TSA processing.

- **Tech Sprints**

FinCEN has previously hosted Tech Sprints, which allow the government, academia, and industry to better understand innovation and the promise of technology in combating money laundering, sanctions evasion, and other forms of illicit finance. Often, FinCEN has coordinated this with other agencies—civil, regulatory, and criminal, and state and federal (and sometimes foreign). These efforts are instrumental in enhancing partnerships, informing stakeholders, and educating and potentially bettering policy choices. Indeed, a Digital Identity Tech Sprint hosted in 2022 by FinCEN and the FDIC challenged participants to develop and demonstrate a "scalable, cost-efficient, risk-based solution to measure the effectiveness of digital identity proofing," and many entries outlined arrangements for structures for public-private partnerships and potential funding arrangements.[36]

FinCEN has also hosted an "Innovation Hours" program, meeting with individual private sector entities to learn about emerging technology within the purview of the BSA or that may

---

[33] Fin. Crimes Enf't Network, FIN-2021-R001, *Exceptive Relief for Casinos from Certain Customer Identity Verification Requirements* (Oct. 19, 2021), https://www.fincen.gov/system/files/administrative_ruling/2021-10-19/Casino%20Exceptive%20Relief%20101921.pdf.

[34] *See* Bd. of Governors of the Federal Reserve, Order (July 31, 2025), https://www.fincen.gov/system/files/2025-08/CIP-TIN-Exemption-Order-Board-only-508.pdf.

[35] Fin. Crimes Enf't Network, *Exemptive Relief Order to Delay the Effective Date of the Investment Adviser Rule* (Aug. 5, 2025), https://www.fincen.gov/system/files/shared/IA-Rule-Exemptive-Relief-Order.pdf.

[36] Fin. Crimes Enf't Network, Press Release, *FDIC FinCEN Digital Identity Tech Sprint – Key Takeaways and Solution Summaries* (Sept. 9, 2022), https://www.fincen.gov/news/news-releases/fdic-fincen-digital-identity-tech-sprint-key-takeaways-and-solution-summaries.

have the potential to support BSA compliance obligations for others. Although these private sector engagement opportunities are constructive, these programs can only have practical effect when coupled with some FinCEN word or action to green light the use of the technology, or provide some type of examination safe harbor for those financial institutions interested in using the technology. Unfortunately, when financial institutions are unwilling to contract with these technology vendors out of fear of an adverse exam finding or an enforcement action, the businesses are handicapped or fail, and the innovation may die too. Thus, coupling such programs with streamlined pilot programs, followed by timely determinations for exceptive relief or guidance to the financial institutions using innovative products, would be most effective.[37]

V. Comments in Response to Certain Research Factors in Question 4(e)

Blockchain-based decentralized identity solutions offer a number of advantages over traditional forms of identification. Of course, these solutions also give rise to risks, but importantly, those risks are generally not novel and already exist in current systems, while the benefits of blockchain-based solutions are significant steps forward from traditional approaches. In other words, the possibility of these risks are far outweighed by the potential benefits of decentralized identity solutions. Indeed, legacy systems of proving identity carry greater risks of fraud, error, and unauthorized dissemination of private information. For these reasons, when addressing risks below, we pair those discussions with an overview of benefits.

A. *Privacy Risks and Benefits*

Decentralized identity generally allows users to selectively disclose personal information, the type of information shared, as well as with whom that information is shared. ZKPs and multi-party computation (MPC) are examples of important technologies that enable such features.[38]

A ZKP is a cryptographic process that allows one party (the prover) to convince another party (the verifier) that a statement is true without revealing information other than the fact that the specific statement is true. (For purposes of this analysis, in many instances the "prover" is the customer, and the "verifier" is the financial institution with which the customer chooses to interact). In other words, a party can prove that a statement is true without having to show why it is true, e.g., that the person is not on the OFAC sanctions list or that he or she is over a certain age.

---

[37] We acknowledge that it would not be appropriate for the U.S. government to "bless" one particular technology or company over another in granting relief or issuing guidance or an administrative ruling, but FinCEN could evaluate categories of technology, operating similarly, or addressing specific compliance objectives, and provide direction or general approval to covered entities on their use in meeting particular BSA obligations.

[38] Notably, in the EU, the eIDAS Regulation encourages integration of ZKP technology into the European Digital Identity Wallet to preserve the privacy of users. *See* Recital 14 of Regulation (EU) 2024/1183. Commentators have noted an advantage of decentralized identity encouraged by the eIDAS Regulation in the EU is that by standardizing attributes and trust services across member states, individuals can access government-run systems across the EU. *See* World Wide Web Consortium, *Use Cases and Requirements for Decentralized Identifiers* (Mar. 17, 2021), at Sec. 2.11, https://www.w3.org/TR/did-use-cases/#publicAuthorityCredentials.

Take the example of proving whether someone is a citizen of a non-sanctioned jurisdiction. Using a ZKP, a person could prove that proposition to someone else without having to disclose a passport, birth certificate, or other information. Moreover, nothing about the data that underlies the personal information need be disclosed, e.g., birthdate, address, or any other information. If a person is, in fact, a citizen of a non-sanctioned jurisdiction, a proof will attest to that fact, or it will fail. ZKPs can be used in many other situations to prove meaningful facts without revealing underlying information. These tools also create cryptographically verifiable audit trails that simplify examinations and investigations. With such minimal and selective disclosures, individuals can verify specific attributes about themselves that are sufficient to satisfy the compliance obligations of third-parties, rather than providing identity documents that include more information than is legally required—a far less invasive method of satisfying compliance requirements.[39]

MPC enables multiple parties that each hold their own private data to jointly compute or evaluate a computation using their private inputs, but without revealing any of the private data held by each party or any other sensitive information.[40] In regard to digital identity credentials, financial institutions could use MPC to assess characteristics about an individual, e.g., their fraud risk, without revealing the private data of that individual to one another.[41] MPC could therefore limit the amount of information that companies must share with one another, as well as with others.

Decentralized identity approaches, like other means of verification, carry some level of risk, and may not be the panacea to every problem. For example, if the underlying proposition to be demonstrated (e.g., "is this potential customer over 18?") can be falsely proven without revealing the underlying information or source of proof, then there might be some opportunities for wrongdoers to commit fraud. Similarly, certain propositions—proof of age, non-inclusion on a sanctions list, qualification as an accredited investor—may be quickly demonstrable by a proof. But others are not. For example, certain inquiries in BSA/AML compliance—such as the legitimacy of one's source of funds, or whether a given transaction or pattern of transactions is lawful—may not be susceptible to easy "proof" in the same way that a more straightforward "yes/no" question might be. There have been proposals in the crypto industry to use ZKP solutions to these questions, but may require additional effort and testing before deployment.[42]

While these limits are real, they should not discourage Treasury from allowing decentralized identity solutions. Even if it is possible that a prover *might* be able to falsely demonstrate a proposition without providing documentary evidence, there is no marginal increase in fraud risk with decentralized identity. And although some AML questions (such as source of funds) may be more judgment-based and complex than others (such as citizenship or age verification), this does not eliminate the utility of decentralized identity. In fact, approaches such as ZKPs and MPC may help demonstrate some of the necessary predication for those more

[39] Van Valkenburgh & Miers, *supra* note 25.
[40] *Privacy-Enhancing Cryptography: Multi-Party Computation (MPC) and Threshold schemes*, NIST (Jan. 3, 2017), https://csrc.nist.gov/Projects/pec/threshold (last updated Sept. 23, 2025).
[41] Van Valkenburgh & Miers, *supra* note 25.
[42] *See, e.g.*, Vitalik Buterin et al., *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium* (Sept. 6, 2023), https://ssrn.com/abstract=4563364 or http://dx.doi.org/10.2139/ssrn.4563364.

complex, multifactor, and judgment-based inquiries. For instance, an individual may be able to demonstrate that she or he has worked in a legal or licensed industry, or has paid taxes, or has banking relationships with a number of banks in regulated institutions. Standing alone, each of these propositions may be unhelpful, but together may assist a financial institution to make other complex, judgment-based determinations about the individual. Moreover, these complex determinations, although difficult, are possibly surmountable, and in any event, worth further exploration given the enormous potential of ZKP, MPC, and other privacy-preserving technologies to address the risks of data overcollection and surveillance.

B. *Improvements in the ability of financial institutions to detect illicit activity involving digital assets and costs to regulated financial institutions*

Decentralized identity has the potential to form the foundation of more efficient and effective AML programs.[43] Financial institutions have extensive AML programs and KYC mechanisms, but those programs and mechanisms have significant drawbacks.

Today, financial institutions collect customer information on an individual basis and retain records that are generally inaccessible to other firms[44]—and sometimes, even to other teams within the firm that collected the information. As a result, financial institutions have to implement extensive AML programs, which include customer due diligence (CDD)[45] (or enhanced due diligence), which includes KYC, and sometimes CIPs[46] and other important features, in order to comply with regulatory obligations. The processes involved in CDD and CIPs are repeated over and over again with the collection of sensitive information, and they can take a significant period of time. After this sensitive information is collected, it is also stored, sometimes across numerous databases.

Reusability. Decentralized identity can solve or mitigate the burden that arises from having to collect significant amounts of customer information on an individual basis because it is reusable. With decentralized identity, financial institutions could use the unique characteristics of blockchains to allow customers to open accounts based on an already-conducted KYC process. For example, a customer could undergo KYC at one financial institution—the initial verifying institution—and receive a token or similar credential attesting to their completion of the process. The customer could then use that token or credential to interact with other financial institutions

---

[43] Paul Grewal, *Ensuring Responsible Development of Digital Assets; Request for Comment*, Coinbase (Nov. 1, 2022), https://assets.ctfassets.net/c5bd0wqjc7v0/4QJpib4JJ4AYCpOiuYavSP/3670f91940053f7e16760d1d74f9051f/Coinbase_Comments_-_Treasury_RFC.pdf.

[44] *See supra* pp. 6-7 (discussing limitations on financial institutions' ability to rely on diligence performed by other financial institutions).

[45] CDD is the process of verifying a customer's identity and "assessing their risk level through background checks, document verification, and monitoring of their business activities to ensure compliance with regulatory requirements and prevent financial crimes." *See Customer due diligence (CDD): An overview*, Thomson Reuters (Feb. 12, 2025), https://legal.thomsonreuters.com/blog/customer-due-diligence-cdd-an-overview/.

[46] For CIPs, financial institutions collect specific identifying information from customers, develop verification procedures focused on uncovering potential risks, establish recordkeeping protocols, and cross-check identifying information against certain government lists. *See Customer Identification Program (CIP): An overview*, Thomson Reuters (Mar. 19, 2025), https://legal.thomsonreuters.com/blog/overview-customer-identification-program-cip/.

to attest that he or she has passed KYC with the initial verifying institution, streamlining the process and ensuring that the customer need not go through the same KYC process at every single institution. The verifying institution could continue to update the token or credential if the customer's risk profile changes, or if additional information is needed, and other financial institutions could set parameters on the types of information that must be included in the token or credential, as well as how up-to-date it must be.[47]

Reducing compliance costs. Reusability also means that institutions do not need to collect as much sensitive personal information, which reduces compliance costs.[48] During the KYC process with the initial verifying institution, the customer could use ZKPs to prove certain information—for instance, that he or she is a U.S. citizen, or is an accredited investor, or is of a certain age—to the verifying financial institution without having to disclose anything else about himself or herself or transmit highly sensitive information. In addition, other institutions that rely on that KYC process do not need to collect any information, which means that institutions do not need to store or have access to data that is not needed for their purposes. Importantly, reusability does come with certain upfront costs, including system integration and training compliance staff. However, following these initial costs, the benefits of reusability should, over time, yield a more cost-effective solution, as well as result in faster onboarding, reduced manual review, and easier integration into transaction monitoring than legacy systems.

Making identity verification less burdensome and more effective. Decentralized identity can make identity verification processes less burdensome and more effective—at the same time. The existing AML regime, described above, has not been effective in deterring illicit finance. A 2011 United Nations report estimated that the "interception rate" for anti-money laundering efforts on a global level is low, appearing that "much less than 1% (probably around 0.2%) of the proceeds of crime laundered via the financial system are seized and frozen."[49] The report notes that its estimates must be "treated with caution," but other researchers have estimated similar numbers.[50] In addition, AML programs generally rely on information collected at the time of onboarding, which does not get updated enough over time. Decentralized identity allows for dynamic, rather than static, risk assessments, which creates an opportunity for updatable proofs and risk assessments that can change over time. Moreover, with decentralized identity, suspicious activity reports and currency transaction reports can be generated automatically and delivered in real time.

---

[47] *See* Grewal, *supra* note 43, at 14-16.
[48] 98% of institutions have reported an increase in financial crime compliance costs. Estimates suggest that the total cost of financial crime compliance is approximately $206 billion globally, with North America comprising approximately $61 billion of that figure. Antonie Bassi & Emilie Beaud, *True Cost Of Financial Crime Compliance Study, 2023*, Forrester, at 9 (Sept. 2023), https://risk.lexisnexis.com/-/media/files/financial%20services/research/lnrs-tlp-true%20cost%20of%20financial%20crime%20compliance_2023.pdf.
[49] *See* United Nations Office on Drugs and Crime, Research Report, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, at 4 (Aug. 31, 2011), https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf.
[50] Van Valkenburgh & Miers, *supra* note 25.

C. *Effectiveness of the methods, techniques, or strategies at mitigating illicit finance*

Current customer information collection processes can involve highly vulnerable security practices, including uploading scans of sensitive physical documents, like passports and driver's licenses. Notably, the physical protections that exist for these documents, such as UV-activated ink patterns, do not have the same effectiveness once scanned and uploaded. Identity theft, fraud, account takeovers, and other similar vectors of attacks, have also been a significant burden on financial institutions for many years.

In 2024, the Federal Trade Commission received more than 1.1 million identity theft reports and millions of other cases of related fraud, with total losses in the billions of dollars.[51] And much of this type of fraud involves victims from vulnerable populations, including the elderly.[52] FinCEN also published a report on identity-related suspicious activity, which found that identity-related BSA reports represented 42% of the approximately 3.8 million reports filed in 2021, equivalent to $212 billion in suspicious activity.[53] In a press release that accompanied the report, FinCEN Director Andrea Gacki stated that, "[t]his report reveals the existence of significant identity-related exploitations through a large variety of schemes," and that "[r]obust customer identity processes are foundational to the security of the U.S. financial system, and critical to the effectiveness of financial institutions' programs to combat money laundering and counter the financing of terrorism."[54] With the proliferation of and improvement in AI tools, the struggle faced by financial institutions regarding identity theft and fraud will increase. For example, generative AI can now produce highly convincing synthetic images, voice samples, and video streams that can defeat remote onboarding and undermine biometric verification.[55]

Decentralized identity is a highly effective tool against identity theft and other similar forms of fraud. Asymmetric or "public-key" cryptography makes it easy to verify ownership of a digital identity, and it ensures that onboarding and ongoing due diligence are tied to cryptographically bound, authoritative attributes rather than unverifiable document scans. And credentials also exist on tamper-proof blockchains in cryptographically secure wallets, which makes them far less susceptible to falsification. Given these characteristics, decentralized identity also helps mitigate against errors in the transmission of information relating to identity.

---

[51] Ben Luthi, *U.S. Fraud and Identity Theft Losses Topped $12.7 Billion in 2024*, Experian (May 30, 2025), https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

[52] *See, e.g.*, Fin. Crimes Enf't Network, *Financial Trend Analysis: Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023* (Apr. 2024), https://www.fincen.gov/system/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf (describing more than $27 billion of suspicious activity associated with elder financial exploitation in a one-year period).

[53] Fin. Crimes Enf't Network, *Identity-Related Suspicious Activity: 2021 Threats and Trends* (Jan. 2024), https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf.

[54] Fin. Crimes Enf't Network, Press Release, *FinCEN Issues Analysis of Identity-Related Suspicious Activity* (Jan. 9, 2024), https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity.

[55] Thankfully, certain blockchain technologies can potentially counter some of these AI risks. *See* Scott Duke Kominers et al., *AI x crypto crossovers*, a16z crypto (June 11, 2025), https://a16zcrypto.com/posts/article/ai-crypto-crossovers/ (discussing forwards-compatible proof of personhood and other identity-related topics).

This reduces the risk of synthetic identity fraud, and therefore, also reduces risks relating to money laundering and sanctions evasion.

D. *Cybersecurity Risks and Benefits*

To be sure and to be fair, any digital identity system (whether centralized or otherwise) dependent upon software and computers is potentially subject to cyber-incidents, whether by accident or design, including intentional wrongdoing (for instance, by hackers). It is possible, for instance, that a decentralized identity solution, if poorly designed, might be exploited, allowing for misuse or corruption of data, potentially leading to fraud or other illicit activity.

But—and also to be sure, and to be fair—the comparative risk of cybersecurity incidents is far lower with decentralized identity. Decentralized identities exist on immutable, decentralized ledgers. As such, they carry substantial advantages over legacy systems: they do not shut down and are always available to their users; and they operate according to predetermined rules that cannot be unilaterally and surreptitiously changed. There is also a lower risk of widespread breaches because there is no single target for hackers, and less susceptibility to failure or mass compromise.

It is also important to consider how traditional centralized third parties hold and store the personal and private information of individuals. As noted above, in many cases, existing online identity tools simply involve companies scanning sensitive identification documents and then sending those documents over unsecured channels, such as email.[56] Not only are these practices inefficient, but they are also potentially dangerous and can result in personal information being stolen, forged, or misused in other ways. Importantly, hacks and other data breaches have resulted in significant leakages of personal information in recent years. In 2023, a Harvard Business Review article estimated that data breaches, in which hackers steal personal data, continued to increase year over year,[57] and a significant market for personal information has proliferated on the Dark Web.[58]

Decentralized identity offers an additional protective layer of security against data breaches and other malicious activity. For one, users hold their credentials in cryptographically secure wallets. In addition, decentralized systems distribute information across a blockchain network, in contrast to traditional systems that store user information and data in centralized databases. While traditional centralized systems create a serious risk of honeypots, decentralized blockchains eliminate single points of failure, thereby reducing the need for centralized databases, as well as the storage of personal information and data across multiple entities.[59] As a

[56] Tyrone Lobban & George Kassis, *Digital identity — The big shift*, kinexys by J.P. Morgan (2022), https://www.jpmorgan.com/kinexys/documents/digital-identity-the-big-shift.pdf.
[57] Stuart Madnick, *Why Data Breaches Spiked in 2023*, Harvard Business Review (Feb. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023.
[58] Ben Luthi, *Here's What Your Data Sells for on the Dark Web*, Experian (June 30, 2025), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[59] Indeed, developers in the blockchain ecosystem are also building decentralized data and file storage projects that provide additional benefits with respect to privacy, security, data integrity, and more. *See Cloud Storage Services: Understanding the Decentralized Storage Approach*, Filecoin Blog (Jan. 26, 2023),

result, the sort of hacks and data breaches that have become all too commonplace for traditional systems are less likely to occur on blockchains.

E. *Other Relevant Factors*

Availability, Scalability, and Interoperability. Blockchains can support billions of identities across the world, and those identities can be used across numerous different platforms, services, and applications. As of 2021, around 850 million people lacked official identification, while many more do not have digitally verifiable identification.[60] Having a decentralized digital identity can help provide users with a secure and efficient form of identification.

Trustless Verification and Censorship Resistance. Blockchains are trustless networks, which means that anyone can cryptographically verify the authenticity of a decentralized identity without having to rely on centralized third-parties. In addition, because blockchains are permissionless and immutable, no one can be excluded from the network or control or revoke someone else's digital identity (although updates can be made in the event of a change).

Assistance to Law Enforcement and the Intelligence Community. Decentralized identity solutions offer extensive benefits, direct and indirect, to government efforts to combat illicit finance, fraud, and other threats to public safety and national security. Some of these are obvious: enabling privacy and enhancing cybersecurity allows individuals and companies to protect themselves from illicit actors. By making sensitive information (including PII and sensitive commercial information) more protected, law enforcement resources can be directed to other efforts.

There are several indirect benefits as well. Law enforcement, regulatory agencies, and the intelligence community have already made extensive use of blockchains in their investigations. Often aided by blockchain analytics tools, law enforcement has been able to interdict and recover proceeds of hacks and exploits; to disrupt the efforts of criminal cartels and hostile foreign state actors; and to identify co-conspirators and networks of criminal organizations. With more robust and reliable evidence of attribution, government investigators and prosecutors will be able to leverage decentralized identity to accurately identify perpetrators and disrupt criminal networks.

Moreover, with prolific use of digital credentials by law-abiding, legitimate users of privacy-enabling technologies, particularly non-custodial and non-BSA obliged blockchains and smart contracts, those technologies may be able to more effectively screen-out bad or sanctioned actors, thus reducing or preventing the ability of those actors to use the privacy-enabling technologies for money laundering and increasing visibility of their transactions to law enforcement.

---

https://filecoin.io/blog/posts/cloud-storage-services-understanding-the-decentralized-storage-approach/#:~:text=Data%20Persistence,provide%20a%20better%20user%20experience. A16z crypto is an investor in Protocol Labs, the developers of Filecoin. *See* https://a16z.com/investment-list/.

[60] ID4D Global Dataset, The World Bank (2021), https://id4d.worldbank.org/global-dataset; *see also* Brett McDowell, *How we create an international framework for privacy-preserving digital ID*, World Economic Forum (Mar. 30, 2023), https://www.weforum.org/stories/2023/03/digital-id-privacy/.

President's Working Group on Digital Asset Markets Recommendations. Finally, alongside our recommendations articulated above, we agree with the President's Working Group's recommendations that Treasury should consider coordinating with NIST and other relevant federal agencies to (1) identify emerging approaches to implement customer identification for digital asset activities; (2) consider and expand upon the results of recent pilot programs and projects, such as the National Cybersecurity Center of Excellence's project for customer identification programs in digital asset activities, as well as state programs; and (3) evaluate existing identity credentialing tools and technical aspects of digital asset services, to determine potential approaches for defining, mandating, and enforcing customer identification programs.[61]

* * *

"The U.S. AML/CFT and sanctions frameworks are designed to protect the integrity of the U.S. financial system on which U.S. persons and the global economy rely for trade, investments, remittances, and everyday transactions."[62] The Bank Secrecy Act and its implementing regulations are also intended to serve important law enforcement goals and to protect national security by ensuring the integrity of the markets, by combating illicit finance, and by preventing the funding of terrorism and proliferation. Millions of Americans, and their global neighbors, are now using emerging technology to conduct their daily activities, including financial activities involving digital assets. In parallel, the illicit finance threat is also changing, and the laws and rules themselves should be stable, but cannot be stagnant. If the United States is to retain its status as the global financial system's leader, then it must lead by example. This leadership requires enabling the adoption of innovative and agile legal and regulatory frameworks, including use of the most cutting edge and effective technologies that developers and entrepreneurs can create. Of equal importance, it also requires recognizing that digital identity could, if implemented incorrectly, have harmful negative consequences, including potential state surveillance, and that therefore, privacy must be a core focus of these developing technologies. As described above, we believe that decentralized solutions are the best pathway for the government to achieve its important objectives while also preserving the freedom and civil liberties of ordinary Americans.

[61] President's Working Grp. on Digital Asset Markets, *Strengthening American Leadership In Digital Financial Technology* (2025), at 111-113, 156. https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.
[62] *Id.*, at 103.

* * *

We greatly appreciate the opportunity to provide comments on these matters and share our expertise, and we respectfully request that the Department consider our recommendations, in particular, the use of its exceptive relief authority to enable financial institutions to deploy decentralized digital identity solutions in furtherance of BSA/AML goals. We look forward to continued engagement with the Department.

Respectfully submitted,

Miles Jennings, Head of Policy & General Counsel
a16z crypto

Michele R. Korver, Head of Regulatory
a16z crypto

Jai Ramaswamy, Chief Legal Officer
a16z

cc: Andrea Gacki, Director of the Financial Crimes Enforcement Network
Tyler Williams, Counselor to the Secretary of the U.S. Department of the Treasury